普通高等教育“十一五”国家级规划教材

信息安全概论

赵俊阁 主编

国家级规划教材

作者权威，学术领先

面向21世纪教学改革

全国优秀出版社倾力打造

国防工业出版社
National Defense Industry Press

普通高等教育“十一五”国家级规划教材

信息安全概论

赵俊阁　主编

国防工业出版社

·北京·

内容简介

在信息时代，各种信息系统的建设、运行极大地解放了生产力，为人类带来了巨大的效益。但同时，信息安全问题也伴随而来。本书全面介绍了信息安全的基本概念、基本原理和基本方法，主要内容包括密码学基础、密码管理及应用、访问控制、恶意代码、数据库安全、安全协议、防火墙与入侵检测、安全评估和信息安全管理等。

本书内容新颖、涵盖全面，既有信息安全的基础理论，又有信息安全的实用技术，文字流畅、表述严谨，并包含了一些信息安全研究的最新成果。

本书适合作为信息安全专业学生的教材，也可供从事相关工作的技术人员和对信息安全感兴趣的读者阅读参考。

图书在版编目(CIP)数据

信息安全概论/赵俊阁主编. —北京：国防工业出版社，2009.7

普通高等教育"十一五"国家级规划教材

ISBN 978-7-118-06267-0

Ⅰ.信… Ⅱ.赵… Ⅲ.信息系统—安全技术—高等学校—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2009)第 041544 号

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

天利华印刷装订有限公司印刷

新华书店经售

开本 787×1092 1/16 印张 17¼ 字数 398 千字

2009 年 7 月第 1 版第 1 次印刷 印数 1—4000 册 定价 30.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)68428422 发行邮购：(010)68414474

发行传真：(010)68411535 发行业务：(010)68472764

前　言

20世纪网络得到了长足的发展，为信息共享提供了平台。信息是社会发展的重要战略资源。信息技术和信息产业正在改变传统的生产、经营和生活方式，成为新的经济增长点。21世纪围绕信息的获取、使用和控制的斗争越演越烈，信息安全成为维护国家安全和社会稳定的一个焦点。

本书在内容上力争做到深入浅出、通俗易懂，略去深奥的数学推导，删减复杂的原理证明。同时具有实用性，既有基础理论知识，又有实用技术；先进性，既有跟踪新进展，又有研究新成果；系统性，既有本学科主干体系，又有多学科交叉知识等。因此，本书适应面较广。

本书共分10章，第1章概要介绍了信息安全、网络安全的基本概念以及信息安全体系和信息安全内容的发展；第2章主要针对信息安全所使用密码技术的常见加密算法及其应用，如数字签名、认证等进行说明；第3章介绍了在密码技术应用中，密钥管理的基本原则和具体方法及证书的具体应用；第4章介绍了安全操作系统的一些基本概念，阐述一些常见的操作系统安全机制，并简要介绍安全操作系统的设计原则和常见操作系统的安全机制；第5章介绍了计算机病毒、网络蠕虫、特洛伊木马等典型恶意代码的特征和基本机理；第6章介绍了数据库安全机制、数据库加密以及Oracle数据库安全问题；第7章介绍了数据链路层安全协议、网络层安全协议、传输层安全协议和应用层安全协议；第8章讲述了防火墙的基本概念，并对防火墙技术以及防火墙的连接和应用等问题进行了一些讨论，然后阐述了入侵检测技术的原理和方法；第9章介绍了从评估标准、评估流程和评估方法与工具如何进行安全评估；第10章从管理原则、管理技术和法律法规上介绍了信息安全管理内容。每章最后附有思考题，供读者学习时使用。

本书由赵俊阁担任主编，黄巍编写第2章，张琪编写第3章，陈泽茂编写第4章、第5章，廖巍编写第6章，薛丽敏编写第7章，魏国珩编写第8章，杜兆将编写第10章，其余由赵俊阁编写并完成了全书的统稿工作。朱婷婷、周立兵、王志锋参加了书稿的讨论。此外，朱婷婷还在本书的整理和文字校对方面做了很多工作。

由于编者水平有限，书中难免有疏漏和错误之处，恳请读者批评指正。

作　者

2008年12月

目　录

第1章 总 论

1.1 基本概念

1.1.1 信息与信息系统

1. 信息的概念

信息一直是人类赖以生存的宝贵资源。在人类社会早期,人们对信息的认识广义而模糊,对信息和消息的含义没有明确的界定。到了20世纪尤其是中期以后,现代信息技术的飞速发展及其对人类社会的深刻影响,迫使人们开始探讨信息的准确含义。

信息的定义是:“作为与物质、能量同一层次的定义,信息就是事物运动的状态与方式。”

信息是事物的一种属性,是一个内容广泛的概念,与其相关的概念有很多,比如知识、消息、信号、数据和情报。信息不同于知识,信息是人类大脑思维的输入,而知识是人类大脑对信息加工形成的结果;信息不同于消息,消息是信息的外壳,信息是消息的内核;信息不同于信号,信号是信息的载体,信息是信号的内容;信息不同于数据,数据是记录信息的一种形式,信息是数据记录的本质,一种信息可以有多种记录形式;信息不同于情报,情报的定义可以从许多方面给出,一般是指在传递中为人们所接受的有用信息。

2. 信息的性质

1)普遍性

根据信息的定义,信息是事物运动的状态和状态改变的方式。只要有事物存在,只要有事物的运动,就会有它们运动的状态和方式,就存在着信息。无论在自然界、人类社会,还是在人的思维领域,绝对的“真空”是没有的,绝对不运动的事物也是没有的,因此,信息是普遍存在的。否认信息的普遍性,就不能解释类似于自动控制系统、地球科学等领域的原理。

2)无限性

在整个宇宙时空中,信息是无限的。即使是在有限的空间中,信息也是无限的。一切事物运动的状态和方式都是信息,而宇宙时空中的事物是无限丰富的,因而它们所产生的信息也必然是无限的。即使是在有限的空间中,事物也是无限多样的,而在无限的时间中,事物的发展变化更是无限的,因而信息自然也是无限的。

3)相对性

信息的相对性体现在对于同一个事物,不同的观察者所能获得的信息量可能不同。由于不同的观察者有着不同的观察角度、不同的分析理解甚至不同的认识目的,因此,从同一个事物所获得的信息量可能各不相同。

4)转移性

信息的转移性是指信息可以在时间上或空间中从一点转移到另一点。由于信息是一

种载体或者说是一种外壳，因而就可以通过一定的方法使它在时间上或在空间中进行转移。在时间上的转移称为存储，在空间中的转移称为通信。当然，信息在空间中的转移必然也伴有时间上的转移，因为它在空间中转移的速度是一个有限值。信息可以在时间上和空间中转移，这是一个十分有用的性质，它使人类的知识能够积累和传播，使人与人之间能够进行信息的交流，使人与其环境之间能够保持信息的联系，从而能够更好地认识和改造环境。

5）变换性

信息可以是变换的，它可以以不同的载体和不同的方法来载荷。既然信息是事物运动的状态和方式，而不是事物本身，它就可以负载在其他一切可能的物质载体和能量形式上。

比如逻辑数字0和1，可以表示电流的有和无，可以表示开关的开和关等。只要能够保持“运动的状态和状态改变的方式”不变性，它就不仅可以在各种物质和能量形式之间进行变换，而且可以经受一切不会破坏“信息不变性”的数学变换。信息的这一性质，使人们对信息施行的各种各样的处理和加工成为可能。

6）有序性

信息可以用来消除系统的不定性，增加系统的有序性。本体论层次的信息是事物运动的状态和方式，认识论层次的信息是认识主体所感知和表述的事物运动的状态和方式。获得信息，就可以消除认识主体对于事物运动状态和方式的不定性。一个系统要想从无序状态转变为有序状态，就必须从外界获得信息，这是自组织理论导出的基本结论。信息的这一性质使信息对人类具有特别重要的价值。

7）动态性

信息具有动态性质，一切活的信息都随时间而变化，因此，信息也是有时效、有“寿命”的。信息是事物运动的状态和状态改变的方式，事物本身在不断发展变化，因此，信息也会随之变化。脱离了母体的信息因为不能够再反映变化了的母体的新的运动状态和方式，它的效用就逐渐降低，以至完全失去效用，这就是信息的时效性。信息脱离母体的时间长短并不能完全反映信息的寿命，衡量信息的寿命必须同时考虑母体随时间而变化的速度。一旦信息已经不能反映母体实际的运动状态和方式，这个信息的寿命就到了尽头，到这时，它至多只能作为母体运动状态和方式的两种历史记录。所以，人们在获得信息之后，并不能就此满足，更不能一劳永逸，信息要及时发挥效用，知识要不断补充更新。

8）转化性

从潜在的意义上讲，信息是可以转化的。它在一定的条件下，可以转化为物质、能量、时间及其他形式。信息可以转化，这当然需要条件，其中最主要的条件就是信息必须被人们有效地利用。没有这个条件，信息是不可能发生这种转化的。同样，“知识就是力量”也是需要这样的条件的。显然，正确而有效地利用信息，就可能在同样的条件下创造更多的物质财富，开发或节约更多的能量，节省更多的时间。

9）共享性

信息可以被众多客体所共享。由于信息可以脱离源事物相对独立地存在并负载于其他载体，因而可以被无限制地进行复制、传播和分配给众多的用户，为大家所共享。因为

信息具有这个特征，所以一个信息持有者把它的信息传递给另一个用户的时候，他自己所拥有的信息并不会丧失。信息的这种特征，使它对人类具有特别重要的意义。而由于物质与能量不具有相对独立性，就不能被共享。

10）客观性

信息是具体的，并且可以被人（生物、机器等）所感知、提取、识别，可以被传递、存储、变换、处理、显示、检索和利用。

信息不是虚无缥缈的东西，也不是可以随意想象和“创造”的事物。它是现实世界各种事物运动的状态和状态改变的方式，具有非常具体和真实的品格。信息可以被感知，人的感觉器官就是专门用来感知信息的，所以被称为信息的感受器官；信息还可以被传递、处理和利用。

信息安全技术关注信息上述性质的相关问题。

3. 系统的概念

系统的概念是信息系统基础概念。一般来说，系统是由一些元素组成的，这些元素之间存在着密切的联系，通过这些联系达到某种目的。

美国国家标准协会（ANSI）对系统的定义是：各种方法、过程或技术结合在一起，按一定的规律相互作用，以构成一个有机的整体。

国际标准化组织技术委员会（ISO/TC）对系统的定义是：能完成一组特定功能的，由人、机器以及各种方法构成的有机集合体。

我国科学家钱学森认为：把极其复杂的研制对象称为“系统”，即由相互作用和相互依赖的若干组成结合成的具有特定功能的有机整体，而且这个“系统”本身又是它所从属的更大系统的组成部分。

任何系统都具有一定的结构，否则不成为系统。所谓系统结构是指系统内各元素之间物理上或逻辑上的关系。如各元素在数量上的比例关系、时间中的先后关系、空间中的位置关系等。系统内各元素间的关系有些是静态稳定的，有些是动态变化的。系统中有意义的元素为实体，描述实体特征的变量称为属性，规定时间的实体运动为活动，描述在任何时间形态的变量为状态变量。

系统的功能即系统要达到的目标或要发挥的作用，是系统的基本属性。不同的系统一般具有不同的功能。系统的功能就是接受物质、能量与信息，并进行处理变换，产生并输出结果，这个结果也是物质、能量与信息。

如图 1－1 所示是某机器人自动装配系统的例子。为了降低系统运行过程中人为失误的影响，整个系统完成一件产品的生产过程为：机器运转一次，产生一个部件；机器人取部件并传输至装配站；机器人组装部件。

系统可以是物理的，也可以是逻辑的。逻辑系统可以是概念、思维或观念的有序集合。系统有输入，是指系统接受的物质、能量和信息；系统也有输出，是指系统经变换后产生的另一种形态的物质、能量和信息；系统的变换需要环境，系统的环境是为系统提供输入或接受输出的场所。有系统就有边界，系统的边界是指一个系统区别于环境或另一个系统的界限。一般来说，系统边界的划分既要使边界包含系统的元素、结构及目标所共同涉及的范围，又要在满足系统目标的前提下，使边界包含的内容尽可能少，直至仅包含那些保证完成系统目标的必要部分。

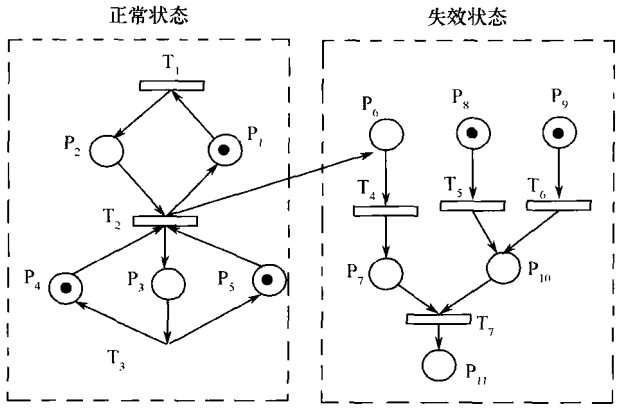

图 1－1　机器人自动装配系统

P_1—机器准备好；P_2—部件存在；P_3—部件在装配站；P_4—装配站未满；

P_5—机器人准备好；P_6—部件意外掉下；P_7—操作员处于危险状态；

P_8—内部锁定即将失效；P_9—电源即将失效；P_{10}—电源没被切断；

P_{11}—系统中断；T_1—机器操作；T_2—机器人取部件并传输至装配站；

T_3—装配；T_4—操作员介入；T_5—内部锁定失效；T_6—电源失效；T_7—事故发生。

4. 信息系统

信息系统是一个集成的系统，任何组织中信息流动的总和构成了一个信息系统，因此，信息系统是根据一定的需要进行输入、系统控制、数据处理、数据存储与输出等活动而涉及到的所有因素的综合体，如图 1－2 所示。

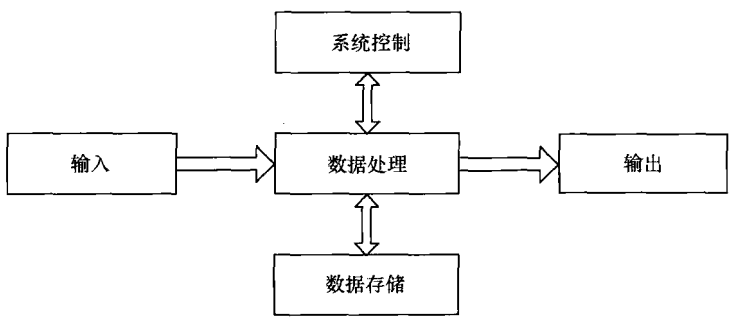

图 1－2　信息系统模型

现代的信息系统一般都是利用计算机来实现的，因此，我们现在所说的信息系统一般是指计算机信息系统或以计算机为基础的信息系统。现代信息系统的构成要素包括人员、硬件、软件、数据 4 种基本资源。

人员包括系统用户和系统专业人员。系统用户是利用信息系统或通过它生产信息的人；系统专业人员包括系统分析人员、程序编写人员与系统操作人员。其中，系统分析人员设计基于用户信息需求的信息系统；程序编写人员根据分析人员的说明书准备计算机程序；系统操作人员负责信息系统的操作。

硬件资源包括计算机系统和载体。计算机系统包括中央处理器及与之相关的外部设备，如图像监控、磁盘驱动器、打印机、光学扫描仪；载体包括存储数据资源用的各种物质材料，如硬盘、磁带、光盘、IC 卡、纸张等。

软件资源包括所有信息处理的指令，不仅包括指示和控制计算机硬件的操作性指令（程序），也包括信息处理的过程指令。程序如操作系统程序、电子表格程序、字处理程序、工资表程序等。过程如数据进入流程、错误改正流程、支票传送流程等。

数据资源包括由数字、字母以及其他字符组成、描述组织活动和其他事情的字母数字型数据；用于书面通信，由句子与段落组成的文本数据；图形和图表形式的图像数据；记录人与其他声音的声频数据。

各种功能的信息系统，已经成为推动社会前进的催化剂和加速器。同时，由于网络的快速普及，处理信息的多样性也使得计算机成为人类社会中一个不可或缺的工具，它为社会各个行业和部门的生产和管理提供了有效的帮助，其提供的多种信息服务，给人类带来了便捷的生活方式。

1.1.2 信息安全

随着计算机在社会各个领域的广泛应用和迅速普及，人类社会步入信息时代，以计算机为核心的各种信息系统建设如雨后春笋，而同时，信息安全问题也伴随而来。信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学等多种学科的边缘学科，影响信息的转移性、变换性、有序性、转化性和动态性。而不良信息散布的问题也属于信息安全问题。

1. 信息安全的概念

信息安全的概念有多种表述。

国际标准化委员会定义的信息安全概念是："为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。"

英国 BS 7799 信息安全管理标准给出的信息安全定义是："信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。"

ISO/IEC 17799 定义信息安全则是通过实施一组控制而达到的，包括策略、措施、过程，组织结构及软件功能，是对机密性、完整性和可用性保护的一种特性。

我国相关立法给出的定义是："保障计算机及其相关的和配套的设备、设施（网络）的安全，运行环境的安全，保障信息安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全。"

国家信息安全重点实验室给出的定义是："信息安全涉及到信息的机密性、完整性、可用性、可控性。综合起来说，就是要保障电子信息的有效性。"

从上述定义中，信息安全包含信息自身的安全，即信息的保密性、完整性、可控性、可用性、不可否认性等存在的问题。信息系统的安全，即信息从产生到运用经历的存储、传输和处理等过程的安全问题。

2. 信息安全属性

信息安全的威胁是通过攻击信息安全属性来达到目的的。在技术层次上安全威胁就是对信息安全属性的破坏。

信息安全的基本属性有：

1)完整性

完整性就是对抗对手主动攻击,防止信息被未经授权的篡改。换言之,完整性是指信息在存储或传输的过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。破坏信息的完整性是对信息安全发动攻击的最终目的。

2)可用性

可用性是指信息可被合法用户访问并能按要求顺序使用的特性,即在需要时就可以取用所需的信息,就是确保信息及信息系统能够为授权使用者所正常使用。

3)机密性

机密性就是对抗对手的被动攻击,保证信息不泄漏给未经授权的人,或者即便数据被截获,其所表达的信息也不被非授权者所理解。

4)可控性

可控性是指授权机构可以随时控制信息的机密性。可控性反映的是信息系统不会被非授权使用,信息的流动可以被选择性阻断。

5)真实性

真实性指信息与信息系统的行为不被伪造、篡改和冒充。真实性反映的是主体身份、行为及相关信息的真实有效。

6)抗抵赖性

抗抵赖性反映的是所生成的信息或信息系统的合法行为不会被否认。

1.1.3 网络安全

1. 网络安全概念

网络安全是指计算机网络系统的硬件、软件及其系统中的数据受到保护,不因偶然或恶意的行为而遭到破坏、更改、泄露,系统连续可靠正常地运行,计算机网络提供的各种服务连续不中断。

网络安全可以理解为有关计算机网络的信息安全问题,计算机网络硬件本身及其运行的数据同样存在着各种各样的安全漏洞和威胁,同样涉及到机密性、完整性、可用性、真实性、可控性和抗抵赖性的相关技术和理论。

对于每个计算机网络用户,总是希望涉及自己的敏感信息在网络上传输时受到机密性、完整性和真实性的保护,希望自己保存在计算机网络系统上的信息不受其他非法用户的非授权访问和破坏,以避免被不希望知道的其他人或对手利用非法手段获取,避免给自己利益和隐私造成损害和侵犯;对于计算机网络管理者,总是希望对于计算机网络信息的访问、读写等操作受到保护和控制,避免出现网络资源不可用、网络系统拒绝服务、计算机及其网络系统感染病毒,避免"黑客"的攻击。

"信息安全"和"网络安全"两个名词非常相似,但是信息安全和网络安全概念的内涵还是有很多的不同,正确认识这两个概念,才能认识到进行全方位信息安全防范工作的重要性。

计算机网络系统包括通常所说的网络资源和信息资源。网络系统包括网络线路和网络设备,信息经过网络资源传输,而且在传输过程中经过包括服务器、客户机、操作系统、外部设备和应用软件等的存储和处理。网络安全考虑的角度主要是如何通过合理的网络