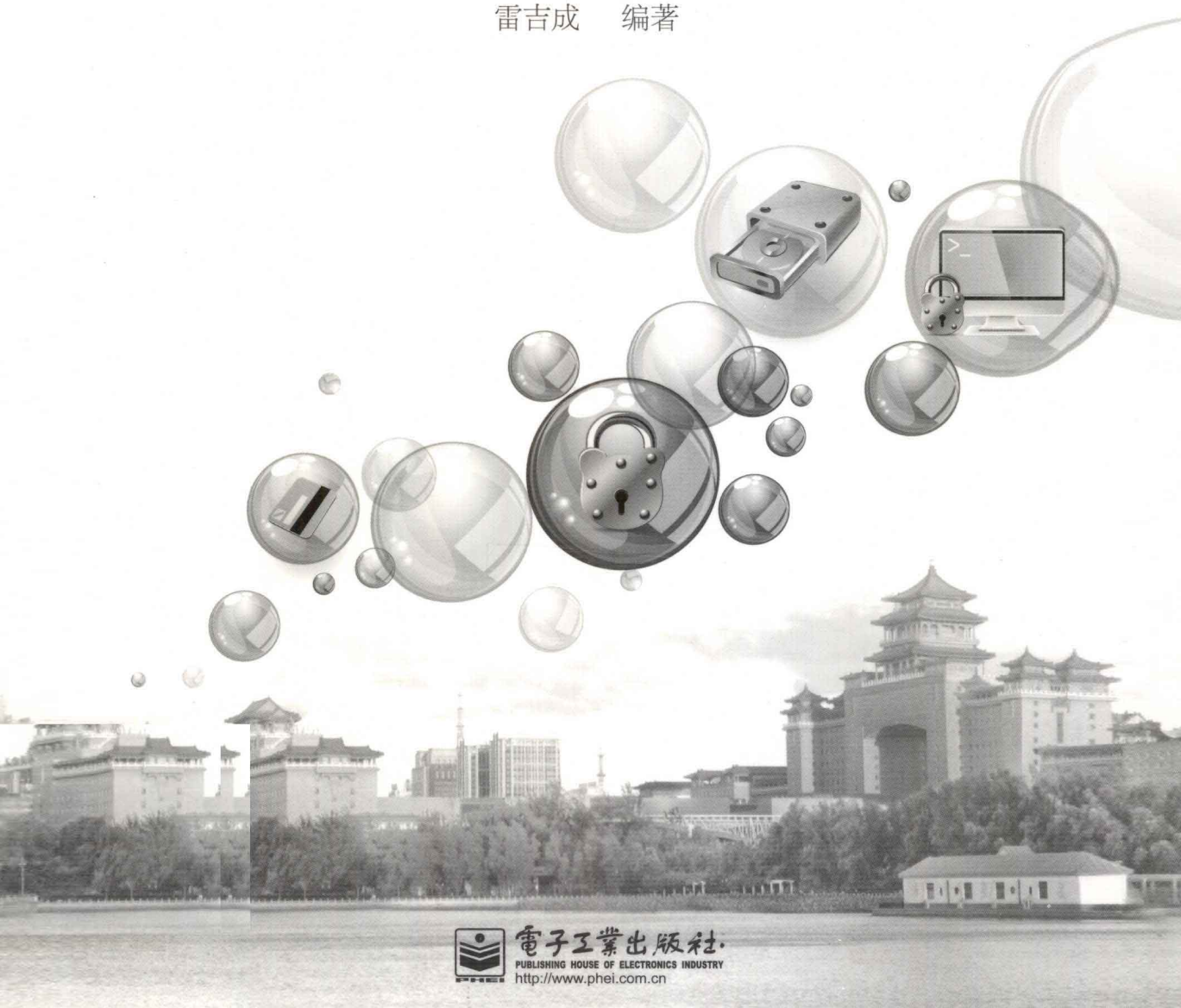
国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

物联网在中国

“十二五”国家重点图书出版规划项目

物联网安全技术

雷吉成　编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

物联网在中国
“十二五”国家重点图书出版规划项目
国家出版基金资助项目

物联网安全技术

雷吉成　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

“物联网在中国”系列丛书编委会名单

EDITORIAL COMMITTEE LIST

“物联网在中国”系列丛书专家顾问委员会

主　任：潘云鹤

副主任：邬贺铨　刘韵洁

委　员：李国杰　何积丰　陈左宁　方滨兴　邓中翰　张文军
朱洪波　郑立荣　熊群力　芮晓武　姜文波

“物联网在中国”系列丛书编写委员会

主　任：张　琪

副主任：敖　然　刘爱民

主　编：潘云鹤

副主编：邬贺铨　刘韵洁

委　员：（以下按姓氏笔画排序）：

马　彦　王　智　王　毅　王立健　王营冠　叶甜春　刘　星
刘风军　刘建明　刘宪兰　刘海涛　刘烈宏　毕开春　许罗德
何　明　吴　巍　吴亚林　吴建平　吴曼青　张　晖　张为民
张学庆　张海霞　李安民　李作敏　李海峰　杨志强　杨放春
肖　波　邹　力　周　翔　周晓鹏　宗　平　欧阳宇　骆连合
俞春俊　洪晓枫　赵立君　倪江波　夏万利　徐勇军　徐晋耀
秦龑龙　郭先臣　顾金星　高燕婕　谢锦辉　蓝羽石　雷吉成
靳东滨　戴定一　魏　凤

FOREWORD 总序

信息技术的高速发展与广泛应用，引发了一场全球性的产业革命，正推动着各国经济的发展与人类社会的进步。信息化是当今世界经济和社会发展的大趋势，信息化水平已成为衡量一个国家综合国力与现代化水平的重要标志。中国政府高度重视信息化工作，紧紧抓住全球信息技术革命和信息化发展的难得历史机遇，不失时机地将信息化建设提到国家战略高度，大力推进国民经济与社会服务的信息化，以加快实现我国工业化和现代化，并将信息产业作为国家的先导、支柱与战略性产业，放在优先发展的地位上。

党的十五届五中全会明确指出：信息化是覆盖现代化建设全局的战略举措；要优先发展信息产业，大力推广信息技术应用。党的“十六大”把大力推进信息化作为我国在21世纪头20年经济建设和改革的一项重要任务，明确要求“坚持以信息化带动工业化，以工业化促进信息化”，“走新型工业化道路”。党的“十七大”进一步提出了“五化并举”与“两化融合发展”的目标，再次强调了走新型工业化道路，大力推广信息技术应用与推动国家信息化建设的战略方针。在中央领导的亲切关怀、指导，各部门、各地方及各界的积极参与和共同努力下，我国的信息产业持续高速发展，信息技术应用与信息化建设坚持“以人为本”、科学发展，取得了利国惠民、举世瞩目的骄人业绩。

近几年来，在全球金融危机的大背景下，各国政要纷纷以政治家的胆略和战略思维提出了振兴本国经济、确立竞争优势的关键战略。2009年，美国奥巴马政府把“智慧地球”上升为国家战略；欧盟也在同年推出《欧洲物联网行动计划》；我国领导在2009年提出了“感知中国”的理念，并于2010年把包含物联网在内的新一代信息技术等7个重点产业，列入“国务院加快培育和发展的战略性新兴产业的决定”中，同时纳入我国“十二五”重点发展战略及规划。日本在2009年颁布了新一代信息化战略 “i-Japan”；韩国2006年提出“u-Korea”战略，2009年具体推出IT839战略以呼应“u-Korea”战略；澳大利亚推出了基于智慧城市和智能电网的国家发展战略；此外，还有“数字英国”、“数字法国”、“新加坡智慧国2015（iN2015）”等，都从国家角度提出了重大信息化发展目标，作为各国走出金融危机、重振经济的重要战略举措。

物联网在中国的迅速兴起绝非炒作。我们认为它是我国战略性新兴产业——信息产业创新发展的新的增长点，是中国信息化重大工程，特别是国家金卡工程最近10年的创新应用、大胆探索与成功实践所奠定的市场与应用基础，是中国信息化建设在更高层面，

向更广领域纵深发展的必然结果。

近两年来，胡锦涛总书记、温家宝总理等中央领导同志深入基层调研，多次强调要依靠科技创新引领经济社会发展，要注重经济结构调整和发展模式转变，重视和支持战略性新兴产业发展，并对建设“感知中国”、积极发展物联网应用等做出明确指示。中央领导在视察过程中，充分肯定了国家金卡工程银行卡产业发展及城市多功能卡应用和物联网 RFID 行业应用示范工程取得的成果，鼓励我国信息业界加强对超高频 UHF 等核心芯片的研发，并就推动物联网产业和应用发展等问题发表了重要讲话，就加快标准制定、核心技术产品研发、抢占科技制高点、掌握发展主动权等，做出一系列重要指示。我们将全面贯彻落实中央领导的指示精神，进一步发挥信息产业对国家经济增长的“倍增器”、发展方式的“转换器”和产业升级的“助推器”作用，促进两化融合发展，真正走出一条具有中国特色的信息产业发展与国家信息化之路。

我们编辑出版“物联网在中国”系列丛书（以下简称“丛书”），旨在探索中国特色的物联网发展之路，通过全面介绍中国物联网的发展背景、体系架构、技术标准体系、关键核心技术产品与产业体系、典型应用系统及重点领域、公共服务平台及服务业发展等，为各级政府部门、广大用户及信息业界提供决策参考和工作指南，以推动物联网产业与应用在中国的健康有序发展。

“丛书”首批 20 分册将于 2012 年 6 月正式发行，我们衷心感谢国家新闻出版总署的大力支持，将“丛书”列入“十二五”国家重点图书出版规划项目，并给予国家出版基金的支持；感谢国务院各相关部门、行业及有关地方，以及我国信息产业界相关企事业单位对“丛书”编写工作的指导、支持和积极参与；感谢社会各界朋友的支持与帮助。谨以此“丛书”献给为中国的信息化事业奋力拼搏的人们！

“物联网在中国”系列丛书编委会

潘雪鹏

2012 年 5 月于北京

前言 PREFACE

物联网，顾名思义，就是将所有物体连接在一起的网络。物体通过二维码、RFID、传感器等信息感知设备与网络连接起来，进行信息交换和通信，实现智能化识别、定位、跟踪、监控和管理。物联网时代，现实的“万物”与虚拟的“网络”将融合为“物联网”，现实的任何物体（包括人）在网络中都有与之对应的“标志”，最终的物联网就是虚拟的、数字化的现实物理空间。

物联网不是对现有技术的颠覆性革命，是现有技术的聚合应用。物联网的核心和基础是网络，是在现有网络基础上延伸和扩展的网络。物联网是互联网发展的延伸。

物联网除了面对传统互联网安全问题之外，还存在着一些与已有互联网安全不同的特殊安全问题。物联网中的“物”信息量比“互联网”时代大很多；物联网的感知设备计算能力、通信能力、存储能力及能量等都受限，不能应用传统互联网的复杂安全技术；现实世界的“物”都连网，通过网络可感知及控制交通、能源、家居等，与人们的日常生活密切相关，安全呈现大众化、平民化特征，安全事故的危害和影响巨大；物联网安全与成本的矛盾十分突出。

互联网中，先系统后安全的思路使安全问题层出不穷，因而物联网应用之初，就必须同时考虑应用和安全，将两者从一开始就紧密结合，系统地考虑感知、网络和应用的安全；物联网时代的安全与信息将不再是分离的，物联网安全不再是“打补丁”，而是要给用户提供“安全的信息”。

本书系统地介绍了物联网安全技术，首先简单介绍信息安全的基本概念和相关技术，然后从物联网的概念和特点开始，分析物联网的安全威胁和安全挑战，以此为基础提出物联网安全的体系结构，然后分别从感知安全、网络安全、应用安全及安全管理等方面说明物联网安全技术，并举例说明了物联网安全的典型应用，最后归纳了物联网安全技术的发展趋势和未来发展方向。

本书由雷吉成研究员编著，陈昌祥负责具体组织和统稿工作。其他参与编写的人员有中国电子科技集团公司第三十研究所喻辉、何恩、黎珂、陈倩、曾梦岐、韦勇刚、林翠萍，卫士通公司胡成华、邓子健，三零凯天公司洪江，三零瑞通公司漆俊峰等。

本书的编写安排如下：

第 1 章，信息安全概述，简单介绍信息安全的基本概念和主要技术，主要由何恩、

喻辉、陈昌祥、黎珂负责编写；

第 2 章，物联网安全概述，概要描述物联网的基本概念和特点，分析其安全威胁和安全需求，提出物联网安全体系结构，简单介绍物联网安全主要的技术，主要由陈昌祥、喻辉、邓子健负责编写；

第 3 章，感知层安全，描述物联网感知的安全需求和相关技术，重点是 RFID 安全和传感器网络安全技术，主要由韦勇刚、林翠萍、曾梦岐负责编写；

第 4 章，网络层安全，描述物联网网络的安全需求和相关技术，包括核心网安全、移动通信接入安全和无线接入系统安全，主要由漆俊峰、曾梦岐负责编写；

第 5 章，应用层安全，描述物联网应用的安全需求和相关技术，主要是数据处理安全、数据存储安全和云安全，主要由曾梦岐、胡成华负责编写；

第 6 章，安全管理支撑系统，描述物联网安全管理的需求、框架和相关技术，主要是安全管理、身份和权限管理，主要由曾梦岐负责编写；

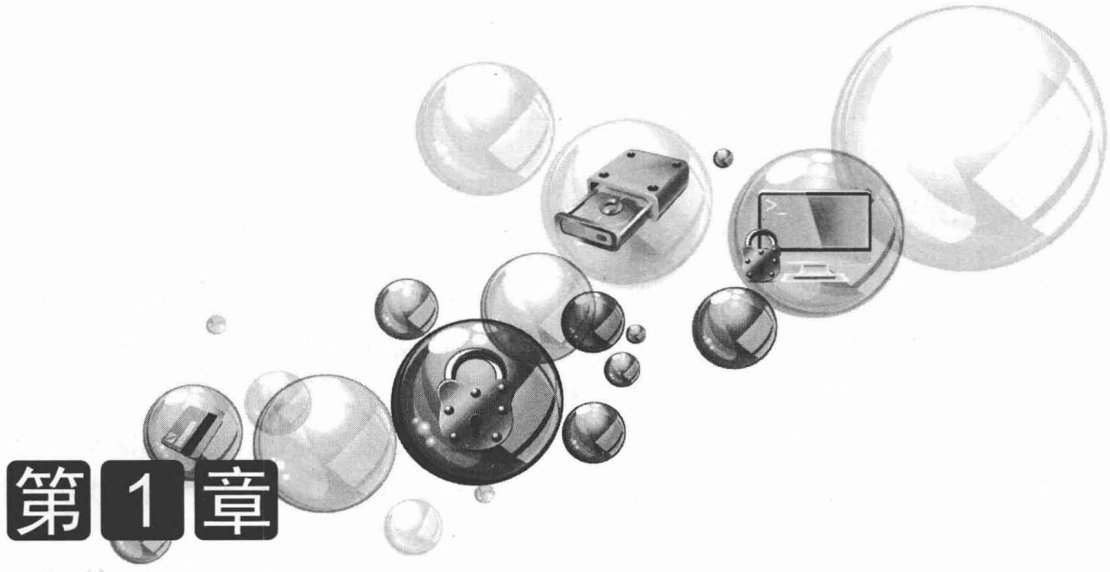
第 7 章，应用案例，举例说明物联网安全的典型应用，包括门禁管理系统安全、贵重物品防伪、安防监控系统安全及智能化监狱系统的安全应用，主要由林翠萍、洪江、漆俊峰负责编写；

第 8 章，物联网安全发展趋势，分析物联网安全技术的发展趋势和发展方向，主要由陈倩负责编写。

对于本书的出版，作者非常感谢中国科学院软件研究所冯登国研究员在百忙之中仔细审阅了本书并给予宝贵的指导，丛书编委会主任张琪女士及电子工业出版社的编辑刘宪兰老师给予大力支持，同时，在本书编辑过程中，三十所周晓明、赵雅丽也给予了大力支持，在此一并表示感谢。

由于作者水平有限，本书难免有缺陷甚至错误，恳请读者给予指正。

CONTENTS 目录



第1章 信息安全概述

内容提要

信息安全（Information Security）涉及信息论、计算机科学和密码学等多方面的知识，它研究计算机系统和通信网络内信息的保护方法，是指在信息的产生、传输、使用、存储过程中，对信息载体（处理载体、存储载体、传输载体）和信息的处理、传输、存储、访问提供安全保护，以防止数据、信息内容或能力被非授权使用、篡改。信息安全的基本属性包括机密性、完整性、可用性、可认证性和不可否认性，主要的信息安全威胁包括被动攻击、主动攻击、临近攻击、内部人员攻击和分发攻击，主要的信息安全技术包括密码技术、身份管理技术、权限管理技术、本地计算环境安全技术、防火墙技术等，信息安全的发展已经经历了通信保密、计算机安全、信息安全和信息保障等阶段。

本章重点

- 信息安全基本属性
- 信息系统面临的风险
- 主要的信息安全技术
- 信息安全的发展阶段

1.1 信息安全概念

在介绍信息安全的概念之前，我们回顾一下生活中发生的信息安全事件。新闻不时报道，某犯罪团伙利用黑客软件盗取了多个银行卡的网银密码，给人们造成经济损失；前几年互联网上的熊猫烧香病毒，影响广泛。

通俗地说，信息安全就是要保护你的网银密码、秘密短信、悄悄电话等不被别人知道，要保护你的计算机不中病毒，保护公众电话网络不被攻击，保护国家铁路、民航等顺利运行。

抽象地说，信息安全是指信息在产生、传输、使用、存储过程中，对信息载体（处理载体、存储载体、传输载体）和信息的处理、传输、存储、访问提供安全保护，以防止数据、信息内容或能力被非授权使用、篡改。

一提信息安全，人们就会想到信息加密，密码技术是信息安全的核心技术，但信息安全不仅仅是加密。比如，对于互联网来说，除了要采用密码技术对网络中的信息进行保护外，还需要实现计算机终端的安全，以及网络设备、通信链路、网络协议、网络应用的安全。

目前，信息安全受到了社会各界的广泛关注。随着人类社会越来越依赖于各种信息，信息安全的重要性日渐突出。信息安全正在渗入人们生活的方方面面，随着物联网概念的提出及物联网应用的日渐增多，人们的日常生活将真正地与信息安全紧密联系在一起。

1.2 信息安全基本属性

信息安全的基本属性有机密性、完整性、可用性、可认证性和不可否认性[1]，也就是说，信息安全的目标是要使得信息能保密，保护信息的完整、可用，确保信息的来源和不可否认。

1.2.1 机密性

机密性是指信息不泄露给非授权的个人和实体或供其使用的特性。只有得到授权或许可，才能得到其权限对应的信息。通常，机密性是信息安全的基本要求，主要包括如下内容。

（1）对传输的信息进行加密保护，防止敌人译读信息并可靠检测出对传输系统的主动攻击和被动攻击。对不同密级的信息实施相应的保密强度和完善及合理的密钥管理。

（2）对存储的信息进行加密保护，有效防止非法者利用非法手段通过获得明文信息来达到窃取机密之目的。加密保护方式一般应视所存储的信息密级、特征和使用资源的

开放程度等具体情况来确定，加密系统应与访问控制和授权机制密切配合，以达到合理共享资源。

（3）防止因电磁信号泄露带来的失密。计算机系统在工作时，常会发生辐射和传导电磁信号泄露现象，若此泄露的信号被敌方接收下来，经过提取处理，就可恢复出原信息而造成泄密。

1.2.2　完整性

完整性，就是要防止信息被非法复制，避免非授权的修改和破坏，以保证信息的正确性、有效性、一致性，或不受意外事件的破坏。

（1）数据完整性。对存储数据的媒体应定期检查其物理操作情况，要尽量减少误操作、硬件故障、软件错误、掉电、强电磁场的干扰等意外事件的发生。要具备检测错误输入等潜在性错误的完整性校验和审计手段。对只需调用的数据，可集中组成数据模块后，使之无法读出和修改。对数据应有容错、后备和恢复能力。数据完整性一般含两种形式：数据单元的完整性和数据单元序列的完整性。前者包括两个过程，一个过程发生在发送实体，另一个过程发生在接收实体。后者主要是要求数据编号的连续性和时间标记的正确性，以防止假冒、丢失、重发、插入或修改数据。

（2）软件完整性。为防止软件被非法复制，对软件必须有唯一的标志，并且能检验这种标志是否存在及是否被修改过。除此之外，还应具有拒绝动态跟踪分析的能力，以免复制者绕过该标志的检验。为防止软件被非法修改，软件应有抗分析的能力和完整性的校验手段。应对软件实施加密处理，这样，即使复制者得到了源代码，也不能进行静态分析。

（3）操作系统的完整性。除计算机硬件外，操作系统是确保计算机安全保密的最基本部件。操作系统是计算机资源的管理者，其完整性控制也至关重要，如果操作系统完整性遭到破坏，也将会导致入侵者非法获取系统资源。

（4）内存完整性、磁盘完整性。为防内存及磁盘中的信息不被非法复制、修改、删除、插入或受意外事件的破坏，必须定期检查内存的完整性和磁盘的完整性，以确保内存磁盘中信息的真实性和有效性。

1.2.3　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。确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。即对于有合法访问权并经许可的用户，不应阻止它们访问那些目标，即不应发生拒绝服务或间断服务。反之，则要防止非法者进入系统访

问、窃取资源、破坏系统；也要拒绝合法用户对资源的非法操作和使用。可用性问题的解决方案主要有如下两种。

（1）避免受到攻击。一些基于网络的攻击被设计用来破坏、降级或摧毁网络资源。解决办法是强化这些资源使其不受攻击。免受攻击的方法包括：关闭操作系统和网络配置中的安全漏洞；控制授权实体对资源的访问；限制对手操作或浏览流经或流向这些资源的数据从而防止带入病毒等有害数据；防止路由表等敏感网络数据的泄露。

（2）避免未授权使用。当资源被使用、被占用或过载时，其可用性会受到限制。如果未授权用户占用了有限的资源（如处理能力、网络带宽、调制解调器连接等），则这一资源对授权用户就是不可用的。识别与认证资源的使用可以提供访问控制来限制未授权使用。然而，过度频繁地发送请求可能导致网络运行减慢或停止。

1.2.4　可认证性

可认证性，是指从一个实体的行为能够唯一追溯到该实体的特性，可以支持故障隔离、攻击阻断和事后恢复等。一旦出现违反安全政策的事件，系统必须提供审计手段，能够追踪到当事人。这要求系统能识别、鉴别每个用户及其进程，能终结他们对系统资源的访问，能记录和追踪他们的有关活动。

通常使用访问控制对网络资源（软件和硬件）和数据（存储的和通信的）进行认证。访问控制的目标是阻止未授权使用资源和未授权公开或修改数据。访问控制运用于基于身份（Identity）和/或授权（Authorization）的实体。身份可能代表一个真实用户、具有自身身份的一次处理（如进行远程访问连接的一段程序）或者由单一身份代表的一组用户（如给予规测的访问控制）。

身份认证、数据认证等可以是双向的，也可以是单向的。要实现信息的可认证性，可能需要认证协议、身份证书技术的支持。

1.2.5　不可否认性

不可否认性，是指一个实体不能够否认其行为的特性，可以支持责任追究、威慑作用和法律行动等。“否认”指参与通信的实体拒绝承认它参加了那次通信。不可否认性安全服务提供了向第三方证明该实体确实参与了那次通信的能力。

不可否认性服务通常由应用层提供，用户最可能参与为应用程序数据（如电子邮件消息或文件）提供不可否认性。在低层提供不可否认性仅能提供证据证明特定的连接产生，而无法将流经该连接的数据同一个特定的实体相绑定。

确保信息交换的真实性和有效性。信息交换的接收方应能证实所收到信息的来源、内容和顺序都是真实的。为保证信息交换的有效性，接收方收到了真实信息时应予以确

认。对所收到的信息不能删除或改变，也不能抵赖或否认。对发送方而言，不能谎称从未发过信息，也不能声称信息是由接收方伪造的。

1.3　信息安全威胁

信息安全所面临的威胁主要包括：利用网络的开放性，采取病毒和黑客入侵等手段，渗透进计算机系统，进行干扰、篡改、窃取或破坏；利用在计算机 CPU（中央处理器）芯片或在操作系统、数据库管理系统、应用程序中预先安置从事情报收集、受控激发破坏的程序，来破坏系统或收集和发送敏感信息；利用计算机及其外围设备电磁泄露，侦截各种情报资料等。

信息系统和网络是颇具诱惑力的受攻击目标。它们抵抗着来自黑客与国家的全方位威胁实体的攻击。因此，它们必须具备限制受破坏程度的能力并在遭受攻击后得以快速恢复。信息保障技术框架[2]认为有以下五类攻击，见表 1-1。

- 被动攻击
- 主动攻击
- 临近攻击
- 内部人员攻击
- 分发攻击

表 1-1　攻击类型

攻 击 类 型	描　　述
被动攻击	被动攻击包括流量分析、监视未受保护的通信、解密弱加密的数据流、获得鉴别信息（如口令）
主动攻击	主动攻击包括企图破坏或攻击系统的保护功能、引入恶意代码及偷窃或修改信息。其实现方式包括攻击骨干网、利用传输中的信息渗透某个区域或攻击某个正在设法连接到一个区域上的合法的远程用户。主动攻击所造成的结果包括泄露或传播数据文件、拒绝服务及更改数据
临近攻击	临近攻击指未授权个人以更改、收集或拒绝访问信息为目的而在物理上接近网络、系统或设备。实现临近攻击的方式是偷偷进入或开放访问，或两种方式同时使用
内部人员攻击	内部人员攻击可以是恶意的或非恶意的。恶意攻击可以有计划地窃听、偷窃或损坏信息；以欺骗方式使用信息，或拒绝其他授权用户的访问。非恶意攻击则通常由粗心、缺乏技术知识或为了“完成工作”等无意间绕过安全策略的行为造成
分发攻击	分发攻击指的是在工厂内或在产品分发过程中恶意修改硬件或软件。这种攻击可能给一个产品引入后门程序等恶意代码，以便日后在未获授权的情况下访问信息或系统

1.3.1　被动攻击

被动攻击包括被动监视公共媒体（如无线电、卫星、微波和公共交换网）上的信息传输。抵抗这类攻击的对策包括使用虚拟专用网 VPN、加密保护网路及使用加保护的分布式网络（如物理上受保护的网络/安全的在线分布式网络）。表 1-2 给出了被动攻击特有的攻击实例。