

信息安全系列丛书

Architecture of Information Security

信息安全体系

王斌君 景乾元 吉增瑞 等 编著

李 昭 刘 舒 审



高等教育出版社

TP309/124

2008

信息安全系列丛书

Architecture of Information Security

信息安全体系

王斌君 景乾元 吉增瑞 等 编著

李 昭 刘 舒 审



高等教育出版社

内容提要

本书以系统论为出发点,从信息安全的技术和管理两个方面详细剖析了信息安全体系的构成,阐述了信息安全体系的基本要素以及相关的技术和管理构件,阐述了它们在信息安全系统中的地位和作用以及它们之间的关联性、互补性,依此建构了信息安全体系的技术框架和管理框架。最后,根据信息安全评估的原理、方法和标准,阐述了信息安全构件和整体的评估。

本书适合信息学科相关专业高年级本科生、研究生以及相关研究人员和工程技术人员阅读。

图书在版编目(CIP)数据

信息安全体系 / 王斌君等编著. —北京:高等教育出版社,
2008.5

ISBN 978-7-04-023984-3

I. 信… II. 王… 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(2008)第 057954 号

策划编辑 陈红英 责任编辑 陈红英 封面设计 刘晓翔 责任印制 韩 刚

出版发行 高等教育出版社
社 址 北京市西城区德外大街 4 号
邮政编码 100120
总 机 010-58581000

经 销 蓝色畅想图书发行有限公司
印 刷 北京民族印刷厂

购书热线 010-58581118
免费咨询 800-810-0598
网 址 <http://www.hep.edu.cn>
<http://www.hep.com.cn>
网上订购 <http://www.landaco.com>
<http://www.landaco.com.cn>
畅想教育 <http://www.widedu.com>

开 本 787 × 1092 1/16
印 张 21.25
字 数 410 000

版 次 2008 年 5 月第 1 版
印 次 2008 年 5 月第 1 次印刷
定 价 36.00 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

版权所有 侵权必究

物料号 23984-00

信息安全系列丛书编审委员会

主 任：卿斯汉

副主任：陈克非 王清贤 王丽娜

委 员(按姓氏笔画排列)：

方 勇	吴 向	李凤华	何大可	张宏丽	张焕国
肖德琴	罗 平	杨义先	杨永川	周明全	林柏钢
赵一鸣	钮心忻	胡华平	贾春福	唐韶华	谢冬青
曾贵华	董晓梅				

前言

随着社会信息化程度的不断提高,信息技术正在深刻影响着人们的生活方式、工作方式乃至整个社会的结构,人类生活和工作已越来越依赖于信息技术。然而,信息技术是一把双刃剑,它在给人类带来文明、便利和进步的同时,也带来了新的安全隐患和威胁:敌对国家和组织利用网络煽动国家分裂、民族矛盾,制造各种政治危机;网络上,各种信息良莠不齐、鱼目混珠、泥沙俱下,流言蜚语、黄色信息充斥;黑客横行,病毒肆虐;信息社会使国家安全和信誉受到严重挑战。信息安全(“领网”)已经成为继陆地、领海、领空之后,国家安全的重要组成部分,倍受世界各国政府和人民的广泛关注,它既是国家意志、政府行为的体现,也需要全社会的广泛参与。

目前,关于信息安全研究的书籍和文章很多,相关的研究机构和公司层出不穷,信息安全产品也林林总总,这些成就总体上主要体现在信息安全的单项技术、单个产品和项目管理的方面。但是,信息安全是一项复杂而庞大的系统工程,仅有这些零零散散的信息安全技术、产品以及相关的安全管理是不够的,需要从系统科学的角度详细分析信息安全的构成,已经有哪些基本的技术和管理要素?还缺哪些要素?这些信息安全要素之间是什么关系?如何由这些信息安全要素构成一个相对完善的信息安全系统?这些问题都是信息安全发展到当前这一阶段急需解决和必须回答的关键问题。

如果将信息安全系统比喻为一张“网格”的话,网络安全问题就是“网格”中“边”的安全问题,显然,还应该“点”的安全问题,即计算机系统上的操作系统和数据库系统等的安全问题,它们作为数据信息存储和处理的节点,才是信息安全的基础和关键所在,对信息的安全保护有着更为重要的作用。

关于本书的框架:本书分4个部分。第1部分基础篇包括第1章、第2章。第1章描述了信息安全的发展轨迹、信息安全的定义、性质、原则和相关的术语以及信息系统的脆弱性和面临的各种威胁。特别是,将信息安全描述为信息本身的安全、处理信息的信息系统安全、信息系统赖以存在环境的物理安全以及使用信息系统和保障物理环境的人的安全,形成本书对信息安全的诠释和界定。第2章以系统科学的思想为指导,遵循信息安全的“木桶原理”,分析了信息安全的构成要素以及要素之间的支撑、关联关系等。第2部分技术篇包括第3章、第4章、第5章,分

别论述信息安全技术的基本要素以及子系统和系统的构成,力图从系统科学的角度论述各信息安全子系统的地位和作用,所包括的主要安全理论和方法以及信息安全技术的整体框架结构。第3部分管理篇包括第6章、第7章、第8章,分别描述了信息安全管理的基本要素,信息安全风险管理的基本理念、方法以及信息安全管理整体框架结构。第4部分评估篇包括第9章、第10章,描述了信息安全的技术框架和管理框架的评估方法及其相关的理论。

王斌君、景乾元和吉增瑞负责本书的整体框架构思和设计。第1章、第4章和第7章由王斌君编写,第2章、第5章由王斌君、景乾元、吉增瑞和李嵩共同编写,第3章由王斌君和王靖亚、孙中庆、李亚丽共同编写,第6章由王斌君和秦力强共同撰写,第8章由王斌君、景乾元和王志强共同编写,第9章、第10章由王斌君和杜彦辉共同撰写,王斌君和吉增瑞负责整本书的统稿工作。

在本书出版之际,对关心和支持我们编写和出版工作的所有同志表示感谢。在本书的写作过程中得到卿斯汉、冯登国、繆道期和杨永川等专家的悉心指导,对他们在本书写作过程中提出的宝贵意见表示诚挚的感谢。同时,对公安大学信息安全专业的苏鹏冲老师,赵雷、李永健、曾旋、王崇、胡存、陈涛等研究生和徐媛媛同学表示感谢,感谢他们在本书的资料收集和整理等方面所做的工作。另外,也感谢相关领导的关心、爱护,感谢家人对我们工作的理解和支持。

由于作者水平有限,欢迎大家多提宝贵意见。

作者

2008年7月于北京

目录

第1部分 基础篇

第1章 信息安全概论	(3)
1.1 信息安全的发展	(3)
1.1.1 信息化的发展历程	(3)
1.1.2 信息安全的发展历程	(5)
1.2 信息安全的内涵	(10)
1.2.1 信息安全的定义	(10)
1.2.2 信息安全的术语	(11)
1.2.3 信息安全的属性	(12)
1.2.4 信息安全的原则	(15)
1.3 信息安全的脆弱性与威胁	(17)
1.3.1 信息安全的脆弱性分析	(18)
1.3.2 信息安全的威胁与分类	(20)
1.3.3 专用网络上的主要安全威胁	(29)
小结	(30)
思考题	(30)
第2章 信息安全的整体性原理	(31)
2.1 整体信息安全的基本原理	(31)
2.1.1 系统的含义	(31)
2.1.2 整体性原理	(34)
2.2 信息安全的整体结构	(35)
2.2.1 信息系统的构成要素	(35)
2.2.2 信息安全的构成要素	(40)
小结	(48)
思考题	(48)

第 2 部分 技术篇

第 3 章 信息安全技术要素	(51)
3.1 物理安全技术的基本内容及定位	(51)
3.1.1 物理安全的定位	(51)
3.1.2 物理安全的基本要素	(51)
3.1.3 物理安全的基本内容	(54)
3.2 密码技术的基本内容及定位	(56)
3.2.1 密码技术的定位	(57)
3.2.2 密码技术的基本原理	(58)
3.2.3 密码技术的应用	(69)
3.3 身份鉴别技术的基本内容及其定位	(78)
3.3.1 身份认证的定位	(78)
3.3.2 身份认证的实现	(79)
3.4 访问控制技术的基本内容及其定位	(80)
3.4.1 访问控制技术的定位	(80)
3.4.2 访问控制的基本内容	(83)
3.4.3 访问控制的模型	(89)
3.4.4 访问控制的实现	(94)
3.5 恶意代码防范技术的基本内容及定位	(96)
3.5.1 恶意代码防范技术的定位	(96)
3.5.2 恶意代码的分类与工作原理	(98)
3.5.3 恶意代码的防范技术	(101)
3.6 风险分析技术的基本内容及定位	(104)
3.6.1 风险分析技术的定位	(105)
3.6.2 风险分析的基本内容	(106)
3.6.3 安全扫描技术	(112)
小结	(123)
思考题	(123)
第 4 章 信息安全子系统	(125)
4.1 安全操作系统	(125)
4.1.1 安全操作系统的地位和作用	(125)
4.1.2 安全操作系统的发展	(127)
4.1.3 安全操作系统的基本内容	(129)

4.2 安全数据库管理系统	(141)
4.2.1 安全数据库管理系统的地位和作用	(141)
4.2.2 安全数据库管理系统的发展	(144)
4.2.3 安全数据库管理系统的基本内容	(146)
4.3 安全网络系统	(159)
4.3.1 安全网络系统的地位和作用	(159)
4.3.2 实用安全协议	(165)
4.3.3 防火墙系统	(170)
4.3.4 VPN 系统	(174)
4.3.5 安全隔离系统	(176)
4.4 信息安全检测系统	(181)
4.4.1 信息安全检测系统的地位和作用	(181)
4.4.2 信息安全检测的发展	(182)
4.4.3 入侵检测系统	(184)
4.4.4 信息内容检测系统	(193)
小结	(197)
思考题	(198)
第5章 信息安全技术体系	(199)
5.1 信息安全的分层技术保护框架	(199)
5.2 信息安全的分域技术保护框架	(201)
5.2.1 局域计算环境安全	(202)
5.2.2 边界安全与信息交换	(203)
5.2.3 网络传输安全	(205)
5.2.4 支撑基础设施	(205)
5.3 信息安全的等级技术保护框架	(206)
5.4 信息安全的过程技术保护框架	(207)
5.4.1 信息系统的安全工程	(208)
5.4.2 信息安全的动态过程保护	(212)
5.5 典型信息安全技术保障框架	(214)
小结	(217)
思考题	(218)
第3部分 管理篇	
第6章 信息安全管理概述	(221)

6.1 管理的基本问题	(221)
6.1.1 管理的概念及特点	(221)
6.1.2 管理的基本手段	(223)
6.1.3 管理的组织结构	(224)
6.2 管理的质量控制	(230)
6.3 信息安全管理概述	(235)
6.3.1 信息安全管理概念	(235)
6.3.2 信息安全管理现状分析	(236)
小结	(240)
思考题	(240)
 第7章 信息安全风险管理	 (241)
7.1 风险管理概述	(241)
7.1.1 风险的基本内容	(242)
7.1.2 风险管理的基本内容	(245)
7.2 风险分析的方法	(248)
7.2.1 定性分析方法	(248)
7.2.2 定量分析方法	(249)
7.3 风险管理	(249)
7.3.1 管理的过程	(250)
7.3.2 管理的角色	(251)
7.3.3 管理的工具	(251)
小结	(252)
思考题	(252)
 第8章 信息安全管理体系	 (253)
8.1 国家层面的信息安全管理体系	(253)
8.1.1 国家层面的组织管理	(253)
8.1.2 国家层面的管理制度	(257)
8.1.3 国家层面的人员管理	(268)
8.1.4 国家层面的监督与检查	(268)
8.2 信息系统层面的信息安全管理体系	(269)
8.2.1 信息系统层面的组织机构	(269)
8.2.2 信息系统层面的管理制度	(271)
8.2.3 信息系统层面的人员管理	(277)
8.2.4 信息系统层面的监督检查	(279)

8.3 信息安全等级保护	(279)
8.3.1 等级保护的基本思路	(279)
8.3.2 等级保护的标准体系	(282)
8.3.3 等级保护的法律保障	(286)
小结	(286)
思考题	(286)
第4部分 评估篇	
第9章 信息安全评估	(289)
9.1 信息安全评估的基本概念	(289)
9.2 信息安全评估的发展	(292)
9.3 典型信息安全评估标准	(293)
9.3.1 TCSEC 标准	(293)
9.3.2 ITSEC 标准	(296)
9.3.3 CC 标准	(298)
小结	(311)
思考题	(312)
第10章 信息系统的安全性评估	(313)
10.1 概述	(313)
10.2 信息系统安全性评估的方法	(315)
10.3 信息系统安全性评估的方式	(317)
10.4 信息系统安全性评估的手段	(318)
10.5 信息系统安全性评估的过程	(319)
小结	(320)
思考题	(321)
参考文献	(322)

第 1 部分 基础篇

信息安全问题由来已久,随着计算机和通信技术的迅猛发展,在网络化的信息社会中,国家机密、企业秘密和个人隐私等信息安全问题显得尤为突出和重要,信息安全已成为国家安全的重要组成部分。

本部分包含两章内容,第 1 章是信息安全概述,描述了信息安全的发展历程以及信息安全的基本概念、相关术语、性质和所遵循的原则以及信息系统的脆弱性和面临的各种威胁,使读者对信息安全的相关问题有一个总体的了解。第 2 章描述信息安全的整体性原理,按照系统化思想,提出信息安全整体性原理和体系,并以信息系统的要素为基础,重点描述了信息安全的构成要素。通过本章的论述,引出第 2 部分技术篇和第 3 部分管理篇的相关内容。

第1章 信息安全概论

随着人类社会迈入信息化时代,计算机、网络和其他 IT 技术日益深刻影响着人们的工作方式、生活方式乃至社会的协作方式和结构,信息与物质和能源一起构成现代社会三大基础和原推动力。然而信息安全是一把双刃剑,它在给人们带来便利的同时,也带来了前所未有的信息安全问题,必须引起高度重视。

1.1 信息安全的发展

1.1.1 信息化的发展历程

信息技术是 20 世纪最伟大的发明之一,它是人类历史上继农业革命、工业革命之后,又一次伟大的变革,被称为“信息革命”、“第三次浪潮”^[10]。信息技术使人类社会在进入 21 世纪之后迈进“信息化社会”。人类社会的发展源于相互沟通、相互交流和相互理解,在计算机、计算机网络和通信等信息技术的推动下,使得一直处于从属和隐蔽地位的信息要素终于显现出来,人类社会从主要依赖于物质和能源,发展到物质、能源和信息三位一体的新时代,信息与物质、能源一起构成社会发展的三大原动力。

1. 国外信息化的发展

信息技术的发展可追溯到 20 世纪 30 年代。1936 年,英国数学家 Turing A. M. 发明了图灵机理论;1937 年,信息论的奠基人香农(Shannon C. E.)在美国麻省理工学院(MIT)发表了《继电器和开关电路的符号分析》硕士论文,奠定了计算机的二进制基础;1945 年,现代计算机之父冯·诺依曼第一次提出了存储程序计算机的概念,形成了现代计算机的计算模型。在这些理论的支撑下,1946 年第一台通用电子计算机 ENAIC 终于在美国宾夕法尼亚州立大学诞生,信息技术进入了一个新时代。1948 年,香农发表的《通信的数学理论》^[8]奠定了现代信息论的基础。

在这一时期,电话、电报、无线电广播和通信技术都得到了长足的发展。到了 20 世纪 60 年代,计算机和通信技术相结合,美国研制并投入使用了 ARPA 网。ARPA 网起初的主要用户是美国军方,后来逐步演化为民用的 DARPA 网。1977 年国际标准化组织(International Standards Organization, ISO)成立了专门的组织,研究

计算机网络问题,并于1984年公布了“开放系统互连基本参考模型”^[34],标准化的研究进一步促进和规范了计算机网络的发展。特别是在1993年,美国宣布建立国家信息基础设施(National Information Infrastructure, NII), Internet(互联网)出现并得到高速发展。目前,互联网已覆盖全球200多个国家,连入互联网的计算机超过4亿台,用户超过5亿人。互联网已将计算机、计算机网络、电话网络以及有线电视网络融为一体,成为国家军事、外交、金融、商业、教育、卫生、娱乐等诸多领域的信息载体。计算机和计算机网络,特别是互联网正在深刻影响着人们的生活方式、工作方式乃至社会的协作方式和结构。

美国政府已投入数百亿美元建设覆盖全国的光纤网络,并准备耗资4 000亿美元,历时20年完成这项宏大的工程。为推进信息化的应用,美国政府提出了“电子政务”的设想,成立了“电子政务特别工作小组”,将电子政务的发展列入每年的财政预算。目前,以计算机和通信技术为核心内容的美国信息产业对美国GDP的贡献已远远超过钢铁、石油、汽车等传统产业,成为美国经济的主导产业。

其他西方国家看准了信息技术对社会发展的重要性,纷纷大力发展自己国家的信息产业。1995年2月25日西方七国召开了部长级会议,讨论全球信息化基础设施(GII)问题,掀起全球信息化建设的高潮。德国政府大力建设155 Mbps的多媒体综合服务网络,目前已铺设8万公里,连接1 500多万户家庭,拥有世界一流的计算机网络信息基础设施。英国政府计划投入380亿英镑,在10年内建成英国的信息高速公路。法国政府每年投入2 000万~2 500万法郎建设法国的综合信息网络。日本政府计划投入45万亿日元,在2015年,将计算机光纤网络连接到日本的每个企业和家庭。

2. 国内信息化的发展

我国的信息化工作开展得相对较晚,20世纪60年代开始起步,由于受到“文化大革命”的影响,信息化工作进展缓慢。20世纪80年代以后,随着国家经济的复苏,信息化工作受到党和国家的高度重视,信息化的研究、应用和普及得到了迅速发展。特别是,随着20世纪90年代互联网技术和全球信息化基础设施建设大环境的影响,我国开展了大规模信息化建设工作。党的十六大提出“坚持以信息化带动工业化,以工业化促进信息化,走出一条科技含量高、经济效益好、资源消耗低、环境污染少、人力资源优势得到充分发挥的新型工业化路子”,将信息化放在战略的高度加以认识和定位。

1993年,中国启动大规模信息化建设的“金桥工程”、“金关工程”和“金卡工程”(统称为“三金工程”)。“金桥工程”是我国信息化的基础设施建设,它以光纤、微波、程控、卫星、无线移动等多种方式形成空、地一体的网络结构,覆盖全国31个省、市、自治区,其中包括500个中心城市、1.2万个大中型企业、100个计划单列的重要企业集团以及国家重点工程,是我国的信息高速公路主干线,并与全球信息高速公路互联。“金关工程”是我国的经济贸易信息网络工程,实现对外贸易的自动

通关和进出口税收等方面的自动化,通过电子数据交换(EDI)对整个国家物资市场流动实行高效管理。“金卡工程”是我国的电子货币工程,在3亿多城市人口中实施金融交易卡,实现了支付手段的革命化变革,并逐步将信用卡发展成为个人与社会的全面信息凭证,如个人身份、经历、储蓄记录、刑事记录等。20世纪末期,我国又相继启动了“金盾工程”、“金税工程”、“金水工程”、“金财工程”、“金审工程”、“金旅工程”、“金保工程”、“金农工程”、“金质工程”和“金信工程”等,形成了我国信息化建设的“十三金”工程。进入21世纪,我国政府与国际接轨,又提出了“电子政务”工程,准备投入数万亿人民币,全面建设政务活动的信息化,以“电子政务”推动“电子商务”的发展,全面实现社会的信息化。

截至2006年底,我国上网用户总数为1.37亿人,占全国人口的10.5%,与上年同期相比,增长率为23.4%,中国网民人数增加了2600万人,是历年来网民增长最多的一年;上网计算机总数达5940万台,其中,宽带上网的网民达到10400万人,占网民总数的75.9%;CN域名总数超过410万个,与2005年同期相比,增长幅度达到64.4%。网站总数达84万多个,网页总数达44亿多个,网页字节数为122306GB;国际出口带宽总量为256696Mbps,仅中国大陆IPv4地址总数就达98015744个($5A+215B+154C$,其中A、B和C分别表示A类、B类和C类地址数)^[14,15]。我国的信息化已进入全面发展阶段,从2002年信息产业占GDP的5.7%,到2006年占GDP的7.5%^①,呈逐年快速增长的态势,信息产业已成为我国最重要的支柱产业。

3. 信息化的内涵

本书的信息是指能输入到计算机中并被加工处理的数字化信息。信息技术(Information Technology, IT)是指在计算机、通信和控制技术支持下,用以获取、加工、存储、变换、显示和传输文字、数据、图像、视频、音频以及语音等信息的技术,是提供设备和信息服务的方法与软、硬件技术的总称。信息技术可表示为: $IT = Computer + Communication + Control$,因此信息技术也称为3C技术。

信息化是指采用信息技术将现实生活中的信息处理变为数字化信息处理的所有活动。这些活动包括组织、管理、技术研发、运行维护、使用和标准化等一系列工作。

总而言之,21世纪是知识经济的时代、信息化的社会。信息化程度标志着一个国家的现代化水平,是一个国家综合实力的体现。信息化主导未来社会的发展方向,谁抢占信息化的制高点,谁就抢占了引领社会发展的先机、拥有“尖端优势”。

1.1.2 信息安全的发展历程

本节首先分析信息安全目前面临的形势,然后回顾信息安全发展的基本历史,最后展望信息安全今后的发展趋势。

^① 信息来源:信息产业部部长王旭东在全国信息产业电视电话会议上的讲话,2006年12月。

1. 信息安全的形势

在信息时代,人们利用计算机和通信网络可以方便地交换信息,提高工作效率,降低成本,提高管理水平。信息化可以创新工作流程,提高对环境变化的快速反应能力。计算机和网络改变了人们的生活方式、工作方式,乃至整个社会的协作模式,涉及政治、经济、国防、教育等国家事务的方方面面,正在深刻影响着人类社会的发展进程。然而,信息技术是一把双刃剑,信息化在给人们带来便利的同时,也产生了大量的、新的、不容忽视的信息安全问题:敌对势力和黑客针对网络上的信息大肆进行攻击、破坏;网上各种信息的真伪难以辨认,在电子政务、电子商务和网上银行等各种信息化活动中,数据的真实性、可靠性无法保障,各种合同纠纷层出不穷;计算机病毒肆意泛滥,网上信息良莠不齐、泥沙俱下、鱼目混珠。国家机密、商业秘密、个人隐私都需要受到保护,信息安全问题在互联网环境中显得尤为突出。

美国有大量的信息安全事件发生,对像美国这样的社会、经济、人民生活严重依赖于信息技术的国家,信息安全事件对其国家安全构成严重威胁,影响了经济的发展和人民的正常生活。美国 9·11 事件以后,美国白宫曾发表了两份报告“National Strategy for the Physical Protection of Critical Infrastructures and Key Assets”和“National Strategy to Security Cyberspace”,将网络空间的安全与现实社会的安全提到对等的高度予以重视,并指出恐怖分子如果利用网络对美国的基础设施和重点保护对象进行任何攻击,其经济损失和社会危害将远远大于 9·11 事件中世贸大楼的影响^[83]。据美国权威机构计算机应急响应小组(Computer Emergency React Team, CERT)的统计,1988—2003 年间共收到各种安全事件 319 992 多起,详细情况如表 1-1 所示。

表 1-1 1988—2003 年信息安全事件统计表

年份/年	安全事件/起	年份/年	安全事件/起
1988	6	1996	2 573
1989	132	1997	2 134
1990	252	1998	3 734
1991	406	1999	9 859
1992	773	2000	21 756
1993	1 334	2001	52 6858
1994	2 340	2002	82 094
1995	2 412	2003	114 855