



“十三五”普通高等教育本科规划教材

信息安全概论

(第二版)

李红娇 主 编
魏为民 李晋国 温 蜜 副主编



中国电力出版社
CHINA ELECTRIC POWER PRESS



“十三五”普通高等教育本科规划教材

信息安全概论

(第二版)

主 编 李红娇
副主编 魏为民 李晋国 温 蜜
编 写 王 勇 袁仲雄 周 林 刘 辉
主 审 李建华



中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书为“十三五”普通高等教育本科规划教材，全书共分12章，主要内容包
括信息安全基础知识、密码学基础、认证与密钥管理技术、访问控制技术、操作系
统安全、数据库安全、计算机网络安全、计算机病毒原理与防范、安全审计、信息
安全管理、信息安全风险评估、面向智能电网的信息安全技术。本书涵盖了信息安
全学科较全面的基础知识，有一定的深度，还具有一定的电力行业特色。

本书可作为普通高等院校本科生和研究生信息安全课程的教材，也可供电力行
业相关技术人员参考。

图书在版编目 (CIP) 数据

信息安全概论/李红娇主编. —2版. —北京: 中国电力出版
社, 2016.4

“十三五”普通高等教育本科规划教材

ISBN 978-7-5123-8868-0

I. ①信… II. ①李… III. ①信息安全-安全技术-高等学校-
教材 IV. ①TP309

中国版本图书馆 CIP 数据核字 (2016) 第 026964 号

中国电力出版社出版、发行

(北京市东城区北京站西街19号 100005 <http://www.cepp.sgcc.com.cn>)

北京市同江印刷厂印刷

各地新华书店经售

*

2012年1月第一版

2016年4月第二版 2016年4月北京第二次印刷

787毫米×1092毫米 16开本 20.25印张 489千字

定价 41.00元

敬告读者

本书封底贴有防伪标签，刮开涂层可查询真伪

本书如有印装质量问题，我社发行部负责退换

版权专有 翻印必究

前 言

本书第一版在 2012 年 1 月出版，该书在过去四年中一直作为一线教学用书，根据四年教学实践中的感悟，以及兄弟院校采用本书作为教材的老师们和读者反馈的信息，加之信息安全技术在迅速发展，为保持“通过具体技术看体系，体现新进展，突出电力特色”的风格本书修订了部分内容。本书的最大变化体现在信息安全技术最近几年的新进展以及面向智能电网的信息安全技术方面。

本书试图从信息安全的体系出发，从基础概念、密码技术、系统安全、网络安全、安全审计、安全管理和安全风险评估等方面逐步理清本学科的脉络，对每个层面的讲述不仅包括基本概念、基本知识、基本技术，还对每种理论与技术介绍了其新进展。最后，将所涉及的信息安全机制应用于智能电网安全。

本书仍保留第一版的篇章结构，第 1 章是信息安全的基本概念和理论方面的内容；第 2~11 章是信息安全学科的代表性安全机制，其中，第 2~3 章介绍密码学，它是信息安全的基础，第 4 章的访问控制技术是信息安全的核心技术之一，第 5~7 章分层次介绍操作系统安全、数据库安全以及计算机网络安全；第 8~11 章分别论述信息系统安全审计，信息安全管理以及安全风险评估技术；而第 12 章的面向智能电网的信息安全技术是多种安全技术的集成应用，前面各章节是它的基础。

在维持基本框架不变的前提下，根据实际发展修订或增加了部分内容。与 2012 年第一版相比，在内容上的主要调整如下：

第 1 章增加信息安全概念的内涵与外延，更新了新技术发展给信息安全带来的新挑战；第 2、3 章更新了密码学的新方向、安全认证和密钥管理的新方向；第 4 章更新了访问控制模型的进展与发展趋势；第 5 章删除了 Windows XP 安全，添加了 Android 系统安全；第 6 章对 SQL Server 数据库的安全机制进行了精简和更新，增加了大数据安全与隐私；第 7 章增加了 APT 攻击与防范以及无线网络安全；第 8 章增加新型计算机病毒 Stuxnet 和手机病毒的内容，以介绍计算机病毒的新发展；第 9 章将取证技术扩展到移动终端；第 10 章针对新型攻击添加了安全威胁情报的内容；第 11 章保留第 1 版的内容；第 12 章是全新的内容。删除了第一版的附录部分。

本书由李红娇担任主编与统稿工作，魏为民、李晋国、温蜜担任副主编。王勇、刘辉、周林对本次教材修订提出了很好的建议，袁仲雄对智能电网信息安全部分的内容给予了很多指导，也经历了上海电力学院信息安全专业和计算机科学技术专业本科生的试用，在编写过程中我们参考了大量著作和教材，这些文献为本书的编写奠定了宝贵的基础，在此对这些文献的作者一并表示衷心的感谢，也感谢第一版所有读者的积极反馈。

编 者

2015 年 12 月于上海

第一版前言

随着互联网应用的日益普及，网络已成为主要的数据传输和信息交换平台，围绕信息的获取、使用、传输引发的安全问题显得越来越重要，信息安全成为维护国家安全和社会稳定的焦点。本书是为高等学校的本科生、研究生提供的了解信息安全概念、原理及技术的一本引导教材。

首先，信息安全是涉及计算机、数学、通信、微电子学等学科的交叉学科，涉及的知识面很广，要处理好各个学科的关系非常不容易。其次，信息安全学科发展非常快，除信息安全的基础知识以外，信息安全的新发展也是学生需要了解的。最后，针对不同的应用环境，信息安全的需求不同，所采用的信息安全架构和机制也会有所不同。

本书试图从信息安全的技术体系出发，从基础概念、密码技术、系统安全、网络安全、安全审计、安全管理和安全风险评估等方面逐步理清本学科的脉络，对每个层面的讲述不仅包括基本概念、基本知识、基本技术，还介绍了每种理论与技术的新进展。从而将基础知识与发展趋势结合，这对启发学生的思考及培养学生的学习与研究兴趣是十分重要的。除介绍通用的信息安全知识和技术外，本书最后还给出了每种安全技术 in 电力信息网络上的应用及实际案例，能让学生将信息安全基础知识、技术与电力信息网络的安全应用结合，从而更深入理解每种安全机制的实质，也有助于学生理论联系实际地从总体上根据实际应用环境把握信息安全体系。

全书共分 12 章。第 1 章简要介绍了信息安全的发展、基本概念、体系结构及信息安全面临的新挑战；第 2 章介绍了密码学的基本概念、重要算法及这些算法在信息安全中的应用；第 3 章介绍了认证技术、密钥管理技术和公钥基础设施；第 4 章介绍了访问控制的基本概念、主要的访问控制模型、访问控制的实施及其新进展；第 5 章介绍了操作系统安全的基本概念、操作系统安全机制及计算机系统安全的新进展——可信计算技术；第 6 章介绍数据库安全的基本概念、数据库的安全机制、主流数据库的安全策略与配置及数据库安全的发展趋势；第 7 章介绍了 Internet 标准的 TCP/IP 模型，主要的网络安全协议、VPN 技术、防火墙技术、入侵检测技术及典型的网络攻击；第 8 章介绍了计算机病毒的概念、分类、感染机制、检测机制、清除机制，以及计算机病毒的新特点；第 9 章介绍了信息系统安全审计的基本概念、关键技术和相关标准，计算机取证是信息系统安全审计的直接应用；第 10 章介绍了保障信息系统安全的信息安全管理，阐述了信息安全管理概念、模型、技术体系、基本方法、保障体系等；第 11 章介绍了安全风险评估的概念、流程、风险评估工具及风险评估技术的新进展；第 12 章介绍了电力信息网络的安全架构及安全机制的设计，讨论了面向智能电网的信息安全技术；在附录中给出了信息安全在电力行业上的实际案例。

本书的建议学时为 40 学时，其中第 1 章 4 学时，第 2 章 6 学时，第 3 章 6 学时，第 4 章 2 学时，第 5 章 2 学时，第 6 章 2 学时，第 7 章 6 学时，第 8 章 4 学时，第 9 章 2 学时，第 10 章 2 学时，第 11 章 2 学时，第 12 章 2 学时。根据各专业的不同教学需求，以上学时安排和内容可根据实际需要进行调整。

本书由李红娇担任主编与统稿工作，温蜜，魏为民担任副主编。李红娇编写了第1章、第4章、第5章、第6章、第8章、第11章和第12章的内容，第2章和第3章由温蜜编写，魏为民编写第7章、第9章和第10章的内容。本书由上海交通大学李建华教授主审。袁仲雄对电力信息网络安全部分的内容给予了很多指导。本书编写过程中，得到了上海市教委科研创新项目（编号12YZ146）、国家自然科学基金青年基金（编号60903188）的资助。在此，一并表示衷心的感谢。

限于编者水平，书中难免有疏漏和不足之处，恳请专家和读者批评指正。

编者

2011年8月于上海

目 录

前言

第一版前言

第 1 章 信息安全基础知识	1
1.1 信息安全的发展历史	1
1.2 信息安全基本概念	6
1.3 信息安全攻击、安全策略与安全机制	9
1.4 信息安全体系结构	14
1.5 新技术发展给信息安全带来的挑战	23
1.6 小结	25
思考题	25
第 2 章 密码学基础	27
2.1 密码学的基本概念	27
2.2 对称密码算法	29
2.3 公钥密码体制	40
2.4 数字签名算法	47
2.5 散列函数	52
2.6 密码学的新方向	55
2.7 小结	57
思考题	57
第 3 章 认证与密钥管理技术	59
3.1 消息鉴别	59
3.2 身份识别	64
3.3 密钥管理技术	71
3.4 密钥管理系统	74
3.5 密钥产生技术	77
3.6 公钥基础设施 (PKI) 管理	78
3.7 安全认证和密钥管理的新方向	84
3.8 小结	84
思考题	85
第 4 章 访问控制技术	86
4.1 访问控制概念	86
4.2 访问控制矩阵	87
4.3 BLP 模型	89
4.4 基于角色的访问控制模型	95

4.5	访问控制实施	101
4.6	访问控制模型新进展及发展趋势	104
4.7	小结	108
	思考题	108
第5章	操作系统安全	110
5.1	基本概念	110
5.2	操作系统面临的安全威胁	112
5.3	操作系统的安全机制	113
5.4	主流操作系统安全	116
5.5	计算机系统安全技术新发展——可信计算	121
5.6	小结	125
	思考题	125
第6章	数据库安全	126
6.1	数据库安全概念	126
6.2	数据库安全需求	127
6.3	数据库安全机制	128
6.4	SQL Server 数据库的安全策略	133
6.5	数据库安全的发展趋势	138
6.6	大数据安全与隐私	138
6.7	小结	143
	思考题	143
第7章	计算机网络安全	145
7.1	TCP/IP 模型	145
7.2	网络安全协议	147
7.3	VPN	157
7.4	防火墙	161
7.5	入侵检测	170
7.6	典型攻击与防范技术简介	177
7.7	无线网络安全技术	191
7.8	小结	201
	思考题	201
第8章	计算机病毒原理与防范	202
8.1	恶意代码	202
8.2	计算机病毒	203
8.3	计算机病毒的工作机制	207
8.4	典型计算机病毒的检测技术	215
8.5	计算机病毒的预防和清除	218
8.6	新型计算机病毒	220
8.7	小结	226

思考题	226
第9章 安全审计	227
9.1 概述	227
9.2 安全审计系统的体系结构	228
9.3 安全审计的一般流程	230
9.4 安全审计的分析方法	231
9.5 安全审计的数据源	233
9.6 信息安全审计与标准	234
9.7 计算机取证	236
9.8 移动终端取证	245
9.9 小结	248
思考题	248
第10章 信息安全管理	249
10.1 信息安全管理概述	249
10.2 信息安全技术体系	253
10.3 信息安全管理方法	255
10.4 信息安全应急响应	257
10.5 安全威胁情报	260
10.6 小结	262
思考题	262
第11章 信息安全风险评估	263
11.1 信息安全风险评估	263
11.2 安全评估标准	264
11.3 风险评估的基本要素	268
11.4 安全风险评估流程	269
11.5 安全风险评估方法	276
11.6 安全风险评估工具	278
11.7 信息安全风险评估技术新进展	281
11.8 小结	282
思考题	283
第12章 面向智能电网的信息安全技术	284
12.1 传统电网与智能电网的区别	284
12.2 智能电网定义	286
12.3 智能电网技术架构	286
12.4 智能电网中的信息安全技术	293
12.5 小结	308
思考题	308
参考文献	309

第1章 信息安全基础知识

信息安全最初是指保护信息系统中处理和传递的秘密数据，随着操作系统、数据库技术和信息系统的广泛应用，信息安全概念从仅侧重机密性扩充到完整性，访问控制技术变得更加重要，因此强调计算机系统安全。网络的发展使信息系统的应用范围不断扩大，要求必须要考虑网络安全。随着云计算等新的信息技术的出现，需要新的思路解决信息安全问题。本章回顾信息安全的发展历史，介绍信息安全基本概念，讲述信息安全攻击、安全策略与安全机制，信息安全体系结构，探讨新技术发展给信息安全带来的新挑战。

1.1 信息安全的发展历史

“信息安全”最初是指信息的保密性。在20世纪的“主机时代”，人们需要保护的主要是设在专用机房内的主机及重要数据，信息安全主要是指信息的保密性、完整性和可用性。20世纪80年代以后，特别是进入20世纪90年代，互联网的飞速发展，使人与计算机的关系发生了质的变化，与此相适应，信息安全的内涵也发生了巨大变化。信息安全既面向数据、设备、网络、环境，也面向使用者，不但包含过去信息安全内涵的延续，例如，面向数据的安全概念拥有前述的保密性、完整性和可用性；还包含新内涵内容的提出，例如，面向使用者、设备、网络、环境的安全概念拥有可控性、不可否认性、可靠性等。目前的信息安全已涉及攻击、防范、监测、控制、管理、评估等多方面的基础理论和实施技术，其中，密码技术和管理技术是信息安全的核心；安全标准和系统评估是信息安全的基础。可以说，现代信息安全是一个综合利用了数学、物理、管理、通信和计算机等诸多学科成果的交叉学科领域，是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共信息安全、国家信息安全的总和。

本节通过对一些重要发展事件回顾，介绍信息安全学科的发展。如图1-1所示，信息安全的发展经历了通信保密、系统安全、网络安全与信息保障及云计算安全等阶段。

1.1.1 通信保密阶段（20世纪40年代—20世纪70年代）

信息安全最初用于保护信息系统中处理和传递的秘密数据，注重机密性，因此主要强调的是通信安全。通信保密阶段以密码学研究为主，重在数据安全层面的研究。密码学的发展历程大致经历了古代加密方法、古典密码和近代密码三个阶段。

1. 古代加密方法

从某种意义上说，战争是科学技术进步的催化剂。人类自从有了战争，就面临着通信安全的需求。密码的使用已有几千年的历史，埃及人是最早使用特别的象形文字作为信息编码的人。早在公元前1世纪，凯撒大帝就曾用过一种代换式密码——Caesar密码。

古代加密方法大约起源于公元前440年古希腊战争中的隐写术。当时为了安全传送军事情报，奴隶主剃光奴隶的头发，将情报写在奴隶的光头上，待头发长长后将奴隶送到另一个部落，再次剃光头发，原有的信息复现出来，从而实现这两个部落之间的秘密通信。密码学

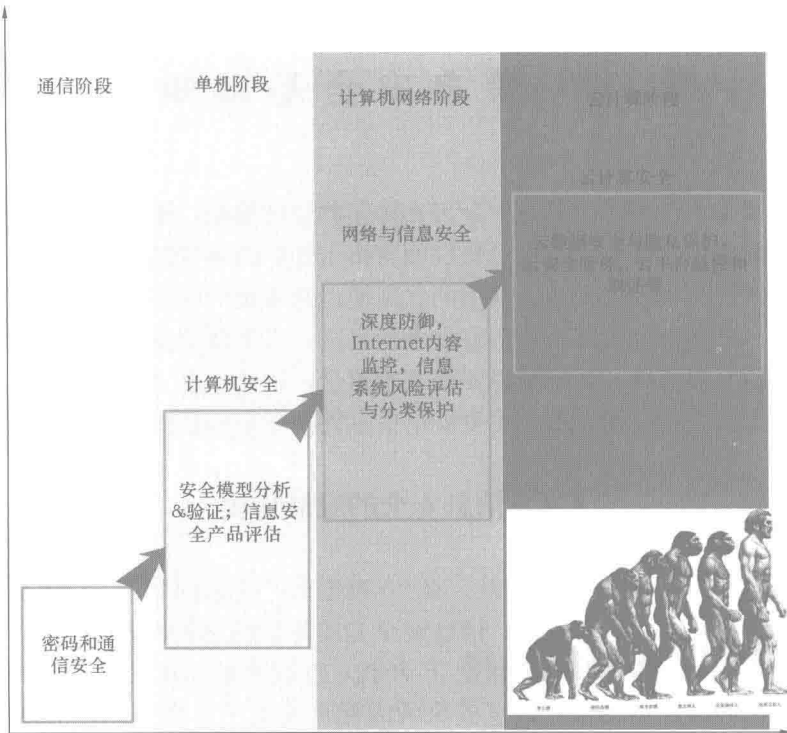


图 1-1 信息安全技术发展阶段图

用于通信的另一个记录是斯巴达人于公元前 400 年应用 Scytale 加密工具在军官间传递秘密信息。Scytale 实际上是一个锥形指挥棒，周围环绕一张羊皮纸，将要保密的信息写在羊皮纸上。解下羊皮纸，则上面的消息杂乱无章、无法理解，但将它绕在另一个同等尺寸的棒子上后，就能看到原始的消息。

由此可见，自从有了文字，人们为了某种需要总是想方设法隐藏某些信息，以起到保证信息安全的目的。这些古代加密方法体现了后来发展起来的密码学的若干要素，但只能限制在一定范围内使用。

古代加密方法主要基于手工的方式实现，因此称为密码学发展的手工阶段。

2. 古典密码

古典密码的加密方法一般是文字置换，使用手工或机械变换的方式实现。古典密码系统已经初步体现出近代密码系统的雏形，它比古代加密方法复杂。古典密码的代表密码体制主要有单表代替密码、多表代替密码及转轮密码。Caesar 密码就是一种典型的单表加密体制；多表代替密码有 Vigenere 密码、Hill 密码；著名的 Enigma 密码就是第二次世界大战中使用的转轮密码。

到了 20 世纪 20 年代，随着机械和机电技术的成熟，以及电报和无线电需求的出现，引起了密码设备方面的一场革命——发明了转轮密码机（简称转轮机，Rotor），转轮机的出现是密码学发展的重要标志之一。几千年来，人们对密码算法的研究和实现主要是通过手工计算来完成的。随着转轮机的出现，传统密码学有了很大的进展，利用机械转轮可以开发出极其复杂的加密系统。1921 年以后的十几年里，Hebern 构造了一系列稳步改进的转轮机，投

入美国海军的试用评估，并申请了第一个转轮机的专利。

德国的 Arthur Scherbius 于 1919 年设计出了历史上最著名的密码机——Enigma 机，英国在第二次世界大战期间发明并使用 TYPEX 密码机，瑞典的 Boris Caesar Wilhelm Hagelin 发明的 Hagelin C-36 型密码机于 1936 年制造，密钥周期长度为 3900255。对于纯机械的密码机来说，这已是非常不简单了。

3. 近代密码

1949 年，信息论创始人 Shannon 发表的论文《保密通信的信息理论》将密码学的研究引入了科学的轨道。1975 年 1 月 15 日，对计算机系统和网络进行加密的数据加密标准 (DES, Data Encryption Standard) 由美国国家标准局颁布为国家标准，这是密码术历史上一个具有里程碑意义的事件。1976 年，当时在美国斯坦福大学的 Diffie 和 Hellman 两人提出了公开密钥密码的新思想 (论文《密码学的新方向》)，把密钥分为加密公钥和解密私钥，奠定了公钥密码学的基础。1977 年，美国的 Ronald Rivest、Adi Shamir 和 Len Adleman 提出了第一个较完善的公钥密码体制——RSA 体制，这是一种建立在大数因子分解基础上的算法，该体制的提出是密码学的一场革命。

(1) 公钥密码体制的理论价值。第一，突破 Shannon 理论，从计算复杂性上刻画密码算法的强度；第二，它把传统密码算法中两个密钥管理中的保密性要求，转换为保护其中一个的保密性，保护另一个的完整性的要求；第三，它把传统密码算法中密钥归属从通信双方变为一个单独的用户，从而使密钥的管理复杂度有了较大下降。

(2) 公钥密码体制在应用上的价值。公钥密码体制提出后的几年，对信息安全应用产生了重要的意义。第一，密码学的研究已经逐步超越了数据的通信保密性范围，同时开展了对数据的完整性、数字签名技术的研究，已成为密码学的最核心部分；第二，随着计算机及其网络的发展，密码学已逐步成为计算机安全、网络安全的重要支柱，使得数据安全成为信息安全的核心内容，超越了以往物理安全占据计算机安全主导地位的状态。

1.1.2 计算机系统安全阶段 (20 世纪 70 年代—20 世纪 80 年代)

自从进入计算机时代，信息安全研究目标扩展到计算机系统安全。在将密码技术应用到计算机通信保护的同时，开始针对信息系统的安全进行研究，重在物理安全层与运行安全层，兼顾数据安全层。随着数据库技术和信息系统的广泛应用，信息安全概念从仅仅侧重机密性扩充到完整性，访问控制技术变得更加重要。20 世纪 70 年代，访问控制技术取得了突破性的成果。同时，信息安全学术界形成了以安全模型分析与验证为理论基础、以信息安全产品为主要构件、以安全域建设为主要目标的安全防护体系思想；不仅涌现出以安全操作系统、安全数据库管理系统、防火墙为代表的信息安全产品，同时形成了相关的信息安全产品测评标准，以及基于安全标准的测评认证制度与市场准入制度，实现了信息安全产品的特殊监管。

1969 年，B. Lampson 提出了访问控制矩阵模型。1973 年，D. Bell 和 L. Lapadula 创立了一种模拟军事安全策略的计算机操作模型 BLP 模型。由于 BLP 模型是针对机密性的，所以，1977 年针对完整性的 Biba 模型被提出，1987 年出现侧重完整性和商业应用的 Clark-Wilson 模型。1996 年出现了 RBAC96、2000 年出现了 NIST RBAC 引用参考标准，权限管理基础设施 (PMI, Privilege Management Infrastructure) 使得访问控制在网络环境下的实施更加方便。

1985年,美国国防部发布可信计算机系统评估准则(TESEC, Trusted Computer Security Evaluation Criteria),即橘皮书。该标准是计算机系统安全评估的第一个正式标准,具有划时代的意义。该准则于1970年由美国国防科学委员会提出,并于1985年12月由美国国防部公布。TCSEC最初只是军用标准,后来延至民用领域。

为了建立一个各国都能接受的通用的信息安全产品和系统的安全性评估准则,1993年6月,美国政府同加拿大及欧共体共同起草单一的通用准则——CC标准(The Common Criteria for Information Technology security Evaluation),并将其推为国际标准。它综合了美国的TCSEC、欧洲的ITSEC、加拿大的CTCPEC、美国的FC等信息安全准则,形成了一个更全面的框架。

我国国家质量技术监督局也于1999年发布了国家标准《计算机信息系统安全保护等级划分准则》(Classified Criteria for Security Protection of Computer Information System),序号为GB 17859—1999,评估准则的制定为评估、开发研究计算机系统安全提供了指导准则。

1.1.3 网络安全与信息保障阶段(20世纪90年代之后)

20世纪60年代开始,美国国防部的高级研究计划局(ARPA, Advance Research Projects Agency)开始建立阿帕网ARPANet, ARPANet就是Internet的前身。Internet的迅猛发展始于20世纪90年代,由欧洲原子核研究组织CERN开发的万维网WWW被广泛使用在Internet上,大大方便了广大非网络专业人员对网络的使用,成为Internet发展的指数级增长的主要驱动力。今天的Internet已不再是计算机人员和军事部门进行科研的领域,而是变成了一个开发和利用信息资源的覆盖全球的信息海洋,覆盖了社会生活的方方面面,构成了一个信息社会的缩影。目前,互联网正从IPv4向IPv6跨越。然而Internet也有其固有的缺点,如网络无整体规划和设计,网络拓扑结构不清晰,以及容错及可靠性的缺乏,而这些对于商业领域的不少应用是至关重要的。安全性问题是困扰Internet用户发展的另一主要因素。计算机病毒、网络蠕虫的广泛传播,计算机网络黑客的恶意攻击,DDOS攻击的强大破坏力、网上窃密和犯罪的增多,使得网络安全性问题关系到未来网络应用的深入发展。当信息技术快速步入网络时代,跨地域、跨管理域的协作不可避免,多个系统之间存在频繁交互或大规模数据流动,专一、严格的信息控制策略变得不合时宜,信息安全领域随即进入了以立体防御、深度防御为核心思想的信息安全保障时代,形成了以预警、攻击防护、响应、恢复为主要特征的全生命周期安全管理,出现了大规模网络攻击与防护、互联网安全监管等各项新的研究内容。安全管理也由信息安全产品测评发展到大规模信息系统的整体风险评估与等级保护等。在这一阶段,开始针对信息安全体系进行研究,重在运行安全与数据安全,兼顾内容安全。

因此,网络安全的研究涉及安全策略、移动代码、指令保护、密码学、操作系统、软件工程和网络安全管理等内容。

1.1.4 信息安全保障

进入20世纪90年代,随着网络技术的进一步发展,超大型网络迫使人们必须从整体安全的角度去考虑信息安全问题。网络的开放性、广域性等特征把人们对信息安全的需求,延展到可用性、完整性、真实性、机密性和不可否认性等更全面的范畴。同时,随着网络黑客、病毒等技术层出不穷、变化多端,人们发现任何信息安全技术和手段都存在弱点,传统“防火墙+补丁”的纯技术方案无法完全抵御来自各方的威胁,必须寻找一种可持续的保护

机制，对信息和信息系统进行全方位的、动态的保护。1989年美国卡内基·梅隆大学计算机应急小组开始研究如何从静态信息安全防护向动态防护转变。之后，美国国防部在其信息安全及网络战防御理论探索中吸收了这一思想，并于1995年提出了“信息保障”概念。信息安全保障在美国称为信息保障（IA，Information Assurance）。1996年美国国防部（DoD）在国防部令S-3600.1中对信息保障下作了如下定义：保护和防御信息及信息系统，确保其可用性、完整性、保密性、可认证性、不可否认性等特性。这包括在信息系统中融入保护、检测、反应功能，并提供信息系统的恢复功能。这就是信息保障的P2DR模型，如图1-2所示。

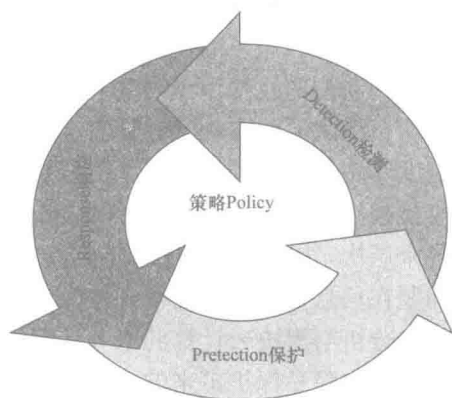


图 1-2 P2DR 模型示意图

信息保障的五个技术环节为预警、保护、检测、响应和恢复。

(1) 预警的概念：根据以前掌握的系统脆弱性和当前了解的犯罪趋势预测未来可能受到的攻击及危害。是否能预警客观存在着空间差、时间差、知识差、能力差的问题。预警的技术支持包括威胁分析、脆弱性分析、资产评估、风险分析、漏洞修补、预警协调。

(2) P（保护，Protect）：采用可能采取的手段保障信息的保密性、完整性、可用性、可控性和不可否认性。技术手段包括网络安全、操作系统安全、数据库系统安全访问控制、口令等保密性和完整性技术。

(3) D（检测，Detect）：利用高级技术提供的工具检查系统存在的可能的黑客攻击、白领犯罪、病毒泛滥等脆弱性。技术手段包括病毒检测、漏洞扫描、入侵检测、用户身份鉴别等。

(4) R（响应，React）：对危及安全的事件、行为、过程及时做出响应处理，杜绝危害的进一步蔓延扩大，力求系统尚能提供正常服务。技术手段包括监视、关闭、切换、跟踪、报警、修改配置、联动、阻断等。

(5) R（恢复，Restore）：一旦系统遭到破坏，尽快恢复系统功能，尽早提供正常的服务。技术手段包括备份、恢复等。

1998年5月美国公布了由国家安全局NSA起草的1.0版本的《信息保障技术框架》（IATF，Information Assurance Technical Framework），旨在为保护美国政府和工业界的信息与技术设施提供技术指南。1999年8月31日IATF论坛发布了IATF2.0版本，2000年9月22日又推出了IATF3.0版本。

1.1.5 云计算安全阶段

云计算以动态的服务计算为主要技术特征，以灵活的“服务合约”为核心商业特征，是信息技术领域正在发生的重大变革。这种变革为信息安全领域带来了巨大的冲击。

(1) 在云平台中运行的各类云应用没有固定不变的基础设施，没有固定不变的安全边界，难以实现用户数据安全与隐私保护。

(2) 云服务所涉及的资源由多个管理者所有，存在利益冲突，无法统一规划部署安全防护措施。

(3) 云平台中数据与计算高度集中，安全措施必须满足海量信息处理需求。

由于当前信息安全领域仍缺乏针对此类问题的充分研究，尚难为安全的云服务提供必要的理论与产品支撑，因此，未来在信息安全学术界与产业界共同关注及推动下，信息安全领域将围绕云服务的“安全服务品质协议”的制定、交付验证、第三方检验等，逐渐发展成一种新型的技术体系与管理体系统之相适应，标志着信息安全领域一个新的时代的到来。从目前来看，实现云计算安全至少应解决关键技术、标准与法规建设，以及国家监督管理制度等多个层次的挑战，下面分别予以简要阐述。

挑战 1：建立以数据安全和隐私保护为主要目标的云安全技术框架。当前，云计算平台的各个层次，如主机系统层、网络层及 Web 应用层等都存在相应安全威胁，但这类通用安全问题在信息安全领域已得到较为充分的研究，并具有比较成熟的产品。研究云计算安全需要重点分析与解决云计算的服务计算模式、动态虚拟化管理方式及多租户共享运营模式等对数据安全与隐私保护带来的挑战。

挑战 2：建立以安全目标验证、安全服务等级测评为核心的云计算安全标准及其测评体系。建立安全指导标准及其测评技术体系是实现云计算安全的另一个重要支柱。云计算安全标准是度量云用户安全目标与云服务商安全服务能力的尺度，也是安全服务提供商构建安全服务的重要参考。基于标准的“安全服务品质协议”，可以依据科学的测评方法检测与评估，在出现安全事故时快速实现责任认定，避免产生责任推诿。

挑战 3：建立可控的云计算安全监管体系。科学技术是把双刃剑，云计算在为人们带来巨大好处的同时也带来巨大的破坏性能力。而网络空间又是继领土权、领空权、领海权、太空权之后的第五维国家主权，是任何主权国家必须自主掌控的重要资源。因此，应在发展云计算产业的同时大力发展云计算监控技术体系，牢牢掌握技术主动权，防止其被竞争对手控制与利用。

1.2 信息安全基本概念

1.2.1 信息安全的定义

信息安全领域的发展历程已多次证明，信息技术的重大变革将直接影响信息安全领域的发展进程。从通信保密到系统安全，从网络安全到信息安全保障，信息安全定义随着网络与信息技术的发展而不断发生变化，其含义也在动态发生变化。

从理念上看，以前信息安全强调的是“规避风险”，即防止发生并提供保护，避免破坏发生时无法挽回；而信息保障强调的是“风险管理”，即综合运用保护、探测、反应和恢复等多种措施，使得信息在攻击突破某层防御后，仍能确保一定级别的可用性、完整性、真实性、机密性和不可否认性，并能及时对破坏进行修复。再者，以前的信息安全通常是单一或多种技术手段的简单累加，而信息保障则是对加密、访问控制、防火墙、安全路由等技术的综合运用，更注重入侵探测和灾难恢复技术。

信息安全逐渐演变成一个综合、交叉的学科领域，不再仅仅限于对传统意义上的网络和计算机技术进行研究，必须要综合利用数学、物理、通信、计算机及经济学等诸多学科的长期知识积累和最新发展成果，进行自主创新研究，并提出系统的、完整的、协同的解决方案。例如，防电磁辐射、密码技术、数字签名、信息安全成本和收益等方面的研究都分别涉及并综合了计算机、物理学、数学及经济学上的一些原理。但是严格来说对信息安全并没有

明确的定义，而只有一些相关的描述。

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。

ISO/IEC 17799 定义信息安全是：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。机密性确保信息只能被授权访问方所接受，完整性即保护信息处理手段的正确与完整，可用性确保授权用户需要在需要时能够访问信息相关资源。

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

从上述定义看，信息安全涵盖两个层次。第一，从信息层次来看，信息安全要保证信息的完整性和保密性。完整性即保证信息的来源、去向、内容真实无误；保密性即保证信息不会被非法泄露与扩散。第二，从网络层次来看，要达到可用性和可控性。可用性即保证网络和信息系统随时可用，运行过程不出现故障，并且在遇到意外情况时能够尽量减小损失，并尽早恢复正常；可控性即对网络信息的传播具有控制能力。

1.2.2 信息安全的内涵与外延

1. 信息空间（CyberSpace）安全

信息空间是自然空间中的一个域，由网络、电磁场以及人在其中的信息交互共同组成，已成为继陆地、海洋、天空和外太空之后人类生存的第五空间，其形成经历了计算机网络安全、电磁与网络融合空间、泛在网络电磁空间三个阶段。

计算机网络空间起始于计算机和网络技术的发展，它的出现不仅是一场科学技术革命，更是人类生活方式革命。20世纪60年代末，“互联网传输控制和网际协议”彻底改变了传统通信传输样式，分组数据包传输以其高效的资源使用率和更大规模的连接能力为计算机网络的出现奠定了基础。随即以有线传输为主的互联网迅速在全球推广并普及，成为人们高度依赖的新平台。

网络技术一经出现，便以惊人的速度发展，朝着网络与电磁融合的方向快速迈进，极大地拓展了人类活动的物理空间。2006年新版美军《联合信息作战条令》写道：“由于无线网络化的不断扩展及计算机与射频通信的整合，使计算机网络战与电子战行动、能力之间已无明确界限。”

仅有50多年历史的网络，以超乎想象的速度在全球推广，成为承载政治、军事、经济、文化的全新空间。特别是随着“网络中心战”“智慧地球”的不断推进，物联网、激光通信、太空互联网、全球信息栅格、云计算技术的发展，使网络与电磁空间融为一体，使网络成为影响社会稳定、国家安全、经济发展和文化传播的重要平台。当前，网络信息层与电磁能量层融合的空间，再一次向认知层和社会层伸出了触角，逐渐形成涵盖物理、信息、认知和社会四域的第五维空间，即泛在的网络电磁空间。

信息空间是一个广泛、无所不在的网络（Ubiquitous and Pervasive Networks），该空间特征为：①网络融合性：互联网、电信网络、广播电视网络、物联网（IoT，Internet of Things）等；②终端多样性：智能手机、电视、PC、IPAD等；③内容多样化：云计算、社交网络、对等网络服务等；④领域广泛性：涉及政治、经济、文化、军事等社会各个层面。

信息空间安全问题。信息空间需要使用动态的资源聚集，这依赖于端对端的连通性和双向的事件通知，导致传统网络安全设施被穿越。信息空间的信息传输往往使用高性能基于UDP的协议，通信源点易于欺骗，这将带来数据传输层的不可靠性。信息空间的扩展性、异构性和动态性等特征带来的诸多安全问题，是现有安全技术无法解决的。我国在打造网络大国的过程中，有责任、有义务保障信息空间的安全、可信和可靠，同时需重点关注以下两方面关键应用需求：①安全问题重心的转移：从低层的信息系统安全向高层的网络平台信息管控转移；②全新的访问控制理论和技术挑战：组织间跨域资源聚合共享。

2. 网络空间安全

网络空间是融合物理域、信息域、认知域和社会域，以互联互通的信息技术基础设施网络为平台，通过无线电、有线电信道传递信号信息，控制实体行为的信息活动空间。网络空间安全包含物理域和信息域两个层面：

(1) 物理域的网络空间安全是指网络空间硬件设施设备安全，要求确保硬件设施设备不被干扰、破坏和摧毁；

(2) 信息域的网络空间安全重点是确保信息的可用性、机密性、完整性和真实性。

在我国，国家高度重视网络空间安全保障工作，网络信息安全上升至国家战略。2014年2月27日中央网络安全和信息化领导小组成立。2015年4月20日《国家安全法（草案）》二审稿增加了国家“建设国家网络与信息安全保障体系，提升网络与信息安全保护能力”、“维护国家网络空间主权”的规定。

1.2.3 安全目标

计算机信息系统的安全目标主要包括机密性、完整性、可用性、不可否认性和身份认证等。其中，机密性、完整性和可用性是信息安全的三个核心安全目标，这五个安全目标对应着五种基本的安全服务。对这五个安全目标的解释随着它们所处环境的不同而不同。在某种特定的环境下，对某种安全目标的解释也是由个体需求、习惯和特定组织的法律所决定的。

1. 机密性

NIST关于机密性的定义：机密性是指对信息或资源的隐藏。信息保密的需求源自计算机在敏感领域的使用，如政府或企业。即机密性指确保信息资源仅被合法的用户、实体或进程访问，使信息不泄露给未授权的用户、实体或进程。

2. 完整性

NIST关于完整性的定义：完整性指的是数据或资源的可信度，通常使用防止非授权的或者未经授权的数据改变来表达完整性。完整性指信息资源只能由授权方式或以授权的方式修改，在存储或传输过程中不丢失、不被破坏。完整性的破坏一般来自未授权、未预期、无意三个方面。

3. 可用性

NIST关于可用性的定义：可用性是指对信息或资源的期望使用能力。即信息可被合法用户访问并按要求的特性使用而不遭拒绝服务。可用的对象包括信息、服务和IT资源。

4. 不可否认性

不可否认性指信息的发送者无法否认已发出的信息或信息的部分内容，信息的接收者无法否认已经接收的信息或信息的部分内容。无论是授权的使用还是非授权的使用，事后都应该是有据可查的。对于非授权的使用，必须是非授权的使用者无法否认或抵赖的，这应该是