普通高等教育“十二五”规划教材

# 信息安全概论

李红娇　主　编
温　蜜　魏为民　副主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

普通高等教育“十二五”规划教材

# 信息安全概论

主　编　李红娇
副主编　温　蜜　魏为民
编　写　袁仲雄
主　审　李建华

中国电力出版社
CHINA ELECTRIC POWER PRESS

## 内 容 提 要

本书为普通高等教育“十二五”规划教材。全书共分十二章，从信息安全技术体系出发介绍信息安全的基础理论和基本技术，主要内容包括信息安全基本概念、密码基础、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、信息安全管理和信息安全风险评估等信息安全学科的基础知识及其最新进展，最后介绍了电力信息网络安全规划与设计，以及面向智能电网的信息安全技术，并给出了电力信息安全的典型案例。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工程技术人员参考。

**图书在版编目（CIP）数据**

信息安全概论/李红娇主编. —北京：中国电力出版社，2011.10

普通高等教育“十二五”规划教材

ISBN 978-7-5123-2254-7

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

中国版本图书馆 CIP 数据核字（2011）第 216157 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）

汇鑫印务有限公司印刷

各地新华书店经售

*

2012 年 1 月第一版 2012 年 1 月北京第一次印刷

787 毫米×1092 毫米 16 开本 17.75 印张 432 千字

定价 **31.00** 元

# 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，除了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。第三，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。除了介绍通用的信息安全知识和技术，本书最后还给出了每种安全技术在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。

全书共分十二章。第一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；第二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；第三章介绍了认证技术、密钥管理技术和公钥基础设施；第四章介绍了访问控制的基本概念、主要的访问控制模型、防问控制的实施及其新进展；第五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；第六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；第七章介绍了 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；第八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；第九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；第十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的概念、模型、技术体系、基本方法、保障体系等；第十一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；第十二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，其中第一章 4 学时，第二章 6 学时，第三章 6 学时，第四章 2 学时，第五章 2 学时，第六章 2 学时，第七章 6 学时，第八章 4 学时，第九章 2 学时，第十章 2 学时，第十一章 2 学时，第十二章 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。李红娇编写了第一章、第四章、第五章、第六章、第八章、第十一章和第十二章的内容，第二章和第三章由温蜜编写，魏为民编写第七章、第九章和第十章的内容。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）、国家自然科学青年基金（编号 60903188）的资助。在此，一并表示衷心的感谢。

由于编者水平有限，书中难免有疏漏和错误之处，恳请专家和读者批评指正。

编　者

2011 年 8 月于上海

# 目　录

# 第一章 绪 论

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，随着操作系统、数据库技术和信息系统的广泛应用，信息安全概念扩充完整，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，必须考虑网络安全。近年来信息安全又增加了新内容，即面向应用的内容安全。随着云计算等新的计算模式的出现，信息安全技术不断向前发展，也面临新的挑战。本章回顾信息安全的发展历史、介绍信息安全基本概念、讲述信息安全机制、信息安全体系结构，探讨信息安全面临的新挑战。

## 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，它既面向数据、设备、网络、环境，也面向使用者，不但包含以前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；也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。

本节通过一些重要发展事件的回顾，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，密码技术源远流长。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。早在公元前一世纪，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

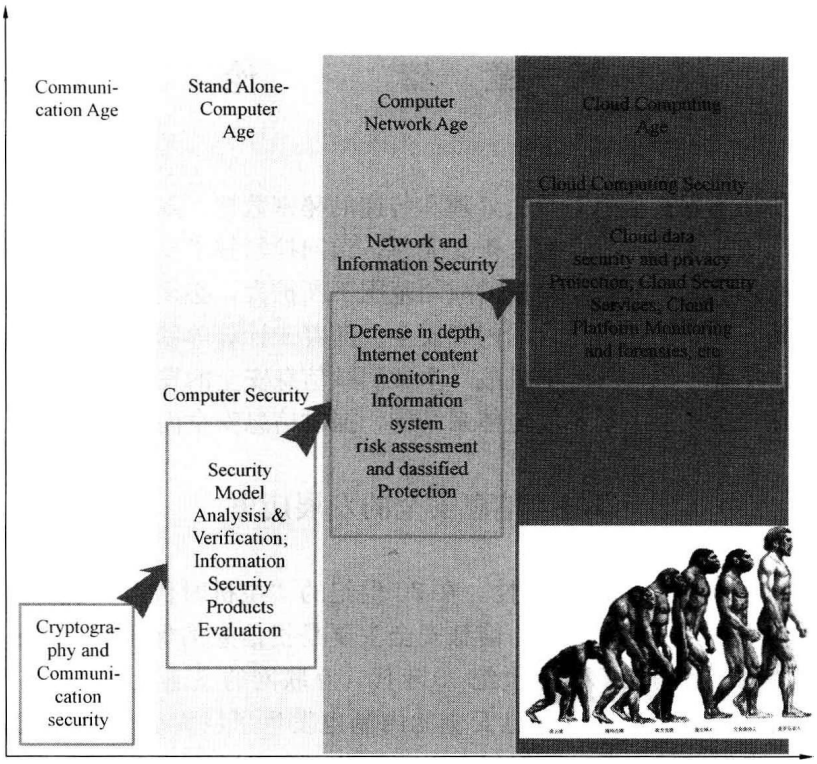


图 1-1 信息安全技术发展阶段图

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，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。

由上可见，自从有了文字以来，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，其变化较小。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，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——德国的 Enigma 机，英国在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迪菲（Diffie）和赫尔曼（Hellman）两人提出了公开密钥密码的新思想（论文“New Direction in Cryptography，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，美国的里维斯特（Ronald Rivest）、沙米尔（Adi Shamir）和阿德勒曼（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，这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两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，已成为最核心的密码；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 年提出了针对完整性的 Biba 模型，1987 年提出了侧重完整性和商业应用的 Clark－Wilson 模型。1996 年提出了 RBAC96、2000 年提出了 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）的国家标准，序号为 GB 17859—1999，评估准则的制定为我们评估、开发研究计算机系统安全提供了指导准则。

### 1.1.3 网络信息安全阶段（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使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，传统的“防火墙＋补丁”这样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，在美国称之为信息保障（IA，Information Assurance）。1996 年美国国防部（DoD）在国防部令 S－3600.1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。

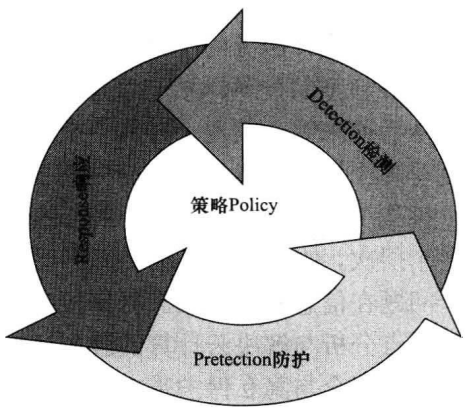


图 1－2 P2DR 模型示意图

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。能不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》（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技术与产品支撑，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，逐渐发展形成一种新型的技术体系与管理体系与之相适应，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、网络层以及 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以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，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、计算机以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 安全目标

计算机信息系统的安全目标主要包括保密性、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

信息安全的最后一个重要环节。

5. 身份认证

认证是安全的最基本要素。信息系统的目的就是供使用者使用的，但只能给获得授权的使用者使用，因此，首先必须知道来访者的身份。使用者可以是人、设备和相关系统，无论是什么样的使用者，安全的第一要素就是对其进行认证。在信息化系统中，对每一个可能的入口都必须采取认证措施，对无法采取认证措施的入口必须完全堵死，从而防堵每一个安全漏洞。

这五种安全目标已经基本上覆盖了现有的攻击。但应当说明的是这五种安全目标绝对没有覆盖未来可能发现的攻击行为。这一点同其他学科不大一样，因为攻、防本身是在不断变化发展的。不同行业、不同用户对于上述安全目标有不同的侧重。

## 1.3 信息安全攻击、安全策略与安全机制

T X.800 标准将常说的“网络安全（Network Security）”进行逻辑上的分别定义，即安全攻击（Security Attack）是指损害机构所拥有信息的安全的任何行为；安全机制（Security Mechanism）是指设计用于检测、预防安全攻击或者恢复系统的机制；安全服务（Security Service）是指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全的服务。三者之间的关系如图 1-3 所示。

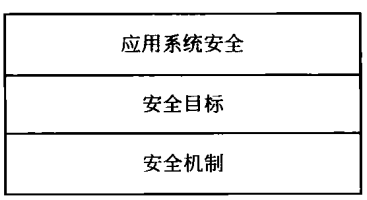


图 1-3 安全体系结构层次

给定一类应用对安全需求归结为一些基本要素，称为安全目标（安全服务），目标通过合理配置安全机制实现。

### 1.3.1 信息安全攻击

信息安全包括机密性、完整性、可用性三个核心目标。根据上述三类安全目标将攻击划分成以下几个分类。

1. 威胁机密性的攻击

（1）窃听。窃听指在未经授权的情况下访问或拦截信息。例如，一个在网络上传输的文件可能含有机密信息，某未经授权的实体就有可能拦截该传输并利用其内容用以牟利。为避免被窃听，通常使用本章中讨论的加密技术，就可以使文件成为对拦截者不可解的信息。

用各种可能的合法或非法手段窃取系统中的信息资源和敏感信息。例如，对通信线路中传输的信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄露截取有用信息等。

（2）流量分析。窃听和数据分析是指攻击者通过对通信线路或通信设备的监听，或通过对通信量（通信数据流）的大小、方向频率的观察，经过适当分析，直接推断出秘密信息，达到信息窃取的目的。例如，可以获得发送者或者接收者的电子地址（如电子邮箱地址），也可以通过收集通信双方的信息来猜测交易的本质。流量分析攻击通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

2. 威胁完整性的攻击

（1）篡改。拦截或访问信息后，攻击者可以修改信息使其对己有利。例如，某客户为一

笔交易给银行发送信息，攻击者即可拦截信息并将其改变为对己有利的交易形式。值得注意的是，有时攻击者只要简单地删除或拖延信息就能给网络造成危害并从中牟利。

(2) 伪装。伪装或欺骗就是攻击者假扮成某人。例如，攻击者伪装为银行的客户，从而盗取银行客户的银行卡密码和个人身份号码。有时攻击者也可能伪装为接收方。例如，当用户设法联系某银行的时候，另外一个地址伪装为银行，从用户那里得到某些相关的信息。

插入、重放指攻击者通过把网络传输中的数据截获后存储起来并在以后重新传送，或把伪造的数据插入到信道中，使得接收方收到一些不应当收到的数据。这种攻击通常也是为了达到假冒或破坏的目的。但是通常比截获/修改的难度大，一旦攻击成功，危害性也大。

(3) 否认。这是一种来自用户的攻击，如否认自己曾经发布过的某条消息、伪造一份对方来信等。

3. 威胁可用性的攻击

威胁可用性的攻击指对信息或其他资源的合法访问被无条件地阻止。典型的威胁可用性的攻击是拒绝服务攻击。拒绝服务攻击的目的是摧毁计算机系统的部分乃至全部进程，或者非法抢占系统的计算资源，导致程序或服务不能运行，从而使系统不能为合法用户提供正常的服务。目前最有杀伤力的拒绝服务攻击是网络上的分布式拒绝服务（DDOS）攻击。

网络拒绝服务是指攻击者通过对数据或资源的干扰、非法占用、超负荷使用、对网络或服务基础设施的摧毁，造成系统永久或暂时不可用，合法用户被拒绝或需要额外等待，从而实现破坏的目的。许多常见的拒绝服务攻击都是由网络协议（如 IP）本身存在的安全漏洞和软件实现中考虑不周共同引起的。例如，TCP SYN 攻击，利用 TCP 连接需要分配的内存，多次同步使其他连接不能分配到足够内存，从而导致系统暂时不可用。

计算系统受到上述类型的攻击可能是黑客或敌手操作实现的，也可能是网络蠕虫或其他恶意程序造成的。典型示例有 SYN Flood 攻击、Ping Flood 攻击、Land 攻击、WinNuke 攻击等。

4. 其他类型的攻击

除了上面明确分类的攻击之外，还存在很多其他类型的攻击，如信息泄露、非法使用(非授权访问)、假冒、旁路控制、授权侵犯、特洛伊木马、陷阱门、计算机病毒、人员不慎、媒体废弃信、物理侵入、窃取、业务欺骗等。这些攻击都不同程度地对系统造成威胁。

5. 主动攻击与被动攻击

根据在系统中的作用，威胁信息系统的攻击可以划分为主动攻击和被动攻击两大类。

(1) 被动攻击（Passive Attack）。在被动攻击中，攻击者的目的只是获取信息，这意味着攻击者不会篡改或危害系统。系统可以不中断其正常运行。然而，攻击可能危害信息的发送者或者接收者。威胁信息机密性的攻击—窃听和流量分析均属于被动攻击。信息的暴露会危害信息的发送者或接收者，但是系统不会受到影响。因此，在信息发送者或接收者发现机密信息已经泄露之前，要发现这种攻击是很困难的。然而，被动攻击可以通过对信息进行加密而避免。

被动攻击主要是收集信息而不是进行访问，数据的合法用户对这种活动一点也不会觉察到。被动攻击包括嗅探、信息收集等攻击方法。报文内容泄露、通信分析法等属于被动攻击。

(2) 主动攻击（Active Attack）。主动攻击可能改变信息或危害系统。威胁信息完整性