“十三五”国家重点出版物出版规划项目

“十三五”江苏省高等学校重点教材　　高等教育网络空间安全规划教材

计算机系统安全原理与技术

第4版

陈波　于泠　编著

http://www.cmpedu.com

电子课件　授课视频　课后习题　教师用课件

机械工业出版社
CHINA MACHINE PRESS

“十三五”国家重点出版物出版规划项目

“十三五”江苏省高等学校重点教材（编号：2016-1-099）

高等教育网络空间安全规划教材

计算机系统安全原理与技术

第4版

陈波　于泠　编著

机械工业出版社

本书全面介绍了计算机系统各层次可能存在的安全问题和普遍采用的安全机制，包括密码学基础、物理安全、操作系统安全、网络安全、数据库安全、应用系统安全、应急响应与灾备恢复、计算机系统安全风险评估、计算机系统安全管理等内容。

本书通过30多个案例引入问题，通过数十个举例帮助读者理解并掌握相关安全原理，还通过17个应用实例进行实践指导。每一章都给出了拓展知识或二维码链接，以及拓展阅读参考文献，并附有思考与实践，总计300多题，题型丰富。全书从正文内容的精心裁剪和组织，到课后思考与实践题的精心设计和安排，为具有高阶性、创新性和挑战度的教学提供帮助，也有助于读者进行深度学习和应用。

本书可以作为网络空间安全专业、计算机科学与技术专业、软件工程专业、信息管理与信息系统专业或相近专业的教材，也可作为信息安全工程师、国家注册信息安全专业人员以及相关领域的科技人员与管理人员的参考书。

本书配有授课电子课件等相关教学资源，需要的教师可登录www.cmpedu.com免费注册，审核通过后下载，或联系编辑索取（QQ：2850823885；电话：010-88379739）。

图书在版编目（CIP）数据

计算机系统安全原理与技术 / 陈波，于泠编著. —4版. —北京：机械工业出版社，2019.12

“十三五”国家重点出版物出版规划项目　高等教育网络空间安全规划教材

ISBN 978-7-111-64618-1

Ⅰ. ①计…　Ⅱ. ①陈…　②于…　Ⅲ. ①计算机安全-高等学校-教材　Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2020)第017713号

机械工业出版社(北京市百万庄大街22号　邮政编码100037)

责任编辑：郝建伟　张翠翠　车　忱

责任校对：张艳霞

责任印制：郜　敏

河北鑫兆源印刷有限公司印刷

2020年3月第4版·第1次印刷

184mm×260mm·25.5印张·629千字

0001-2000册

标准书号：ISBN 978-7-111-64618-1

定价：79.00元

电话服务

客服电话：010-88361066

010-88379833

010-68326294

封底无防伪标均为盗版

网络服务

机　工　官　网：www.cmpbook.com

机　工　官　博：weibo.com/cmp1952

金　　书　　网：www.golden-book.com

机工教育服务网：www.cmpedu.com

高等教育网络空间安全规划教材
编委会成员名单

前　言

在网络空间中，信息的触角延伸到社会生产和生活的每一个角落。每一个网络结点、每一台计算机、每一个网络用户都可能成为信息安全的危害者和受害者。在当前这个“无网不在”的信息社会，网络成为整个社会运作的基础，由网络引发的信息安全担忧成为全球性、全民性的问题。本书介绍的是在网络空间环境下运行的计算机信息系统的安全问题，以及安全控制原理与技术。

本书第3版出版迄今已逾6年，受到了广大读者的欢迎，被数十所高校选为教材使用，发行量在同类教材中名列前茅。但计算机信息系统安全攻防在不断发展，新的安全防护技术和安全思想不断产生，因而本书内容也必须与时俱进。在大家的期待和鼓励下，我们用了近两年的时间完成了本书的修订工作。

本书的修订工作适应国家对网络空间安全高层次人才培养的需求，具有强烈的时代背景和应用价值。2014年为我国信息安全元年。2014年2月27日，中共中央网络安全和信息化领导小组（现已更名为“中共中央网络安全和信息化委员会办公室”）成立，这标志着信息安全已成为构建我国国家安全体系和安全战略的重要组成。习近平总书记指出“没有网络安全就没有国家安全，没有信息化就没有现代化”。2015年6月，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，促使高校网络空间安全高层次人才培养进入了一个新的发展阶段。2016年6月，中央网络安全和信息化领导小组办公室等六部门联合印发了《关于加强网络安全学科建设和人才培养的意见》，对网络安全学科专业和院系建设、网络安全人才培养机制、网络安全教材建设等提出了明确要求。

本书第4版在2016年被国家新闻出版广电总局列入“十三五”国家重点出版物出版规划项目“高等教育网络空间安全规划教材”。该系列教材编委会由我国网络空间安全领域的沈昌祥院士担任名誉主任，上海交通大学网络空间安全学院院长、国家教育部网络空间安全专业教学指导委员会副主任李建华教授担任主任，本书主编陈波教授担任委员。在编委会会议上，专家们对本书的第4版进行了审定，与会专家对该教材给予了高度评价。

本次修订是编者对多年来教学改革成果的总结。本书是江苏省“十三五”高等学校重点教材（修订）、江苏省高等教育教学改革重点课题（2015JSJG034）和一般课题（2019JSJG280）、江苏省教育科学十二五规划重点资助课题（泛在知识环境下的大学生信息安全素养教育——培养体系及课程化实践）、南京师范大学精品课程“计算机系统安全”及南京师范大学“信息安全素养与软件工程实践创新教学团队”建设项目的成果。

本书第4版对前3版进行了全面修订，大部分章节与第3版相比做了较大修改，突出和加强了计算机信息系统安全的新技术，以足够的广度和深度涵盖该领域的核心内容。本书在修订中力求体现以下三大特色。

1. 知识体系完整，章节内容全面

本书基于信息保障模型（PDRR）——保护、检测、响应与恢复的理论，全面介绍了计算机系统各层次可能存在的安全问题和普遍采用的安全机制，包括密码学基础、物理安全、操作系统安全、网络安全、数据库安全、应用系统安全、应急响应与灾备恢复、计算机系统安全风

险评估、计算机系统安全管理等内容。

第 1 章为计算机系统安全概述。从什么是计算机系统讲起，然后介绍计算机系统安全概念的发展，再谈到计算机系统安全问题的产生，以及计算机系统安全问题解决的途径，最后给出计算机系统安全研究的主要内容。其中，增加介绍网络空间安全的概念和内涵以及与计算机系统安全的关系，增加介绍计算机系统安全防护体系，对全书的学习起到提纲挈领的作用。

第 2 章为密码学基础。从密码学基本概念、对称密码算法、公钥密码算法、密钥管理、哈希函数、数字签名和消息认证、密码算法的选择与实现、信息隐藏、密码学研究与应用新进展等多个方面阐述密码学原理与技术应用，不仅补充了这些方面新的理论和技术，尤其增加了密钥管理、密码算法的选择与实现、密码学研究与应用新进展等内容，而且更加强化密码技术的实践与应用。

第 3 章为物理安全。首先分析计算机设备与环境面临的安全问题，然后分别从数据中心物理安全防护、PC 物理安全防护及移动存储介质安全防护展开介绍。其中，增加介绍旁路攻击、设备在线等工业控制系统面临的安全新威胁，并根据新的国家标准重新组织了环境安全技术等内容。

第 4 章为操作系统安全。这一章首先分析了操作系统安全的重要性及操作系统面临的安全问题，然后介绍了操作系统安全及安全操作系统的相关概念，着重介绍了操作系统中的身份认证和访问控制两大安全机制，最后以 Windows 和 Linux 两大常见系统为例，介绍了安全机制在这些系统中的实现。其中，增加了生物特征认证新技术及 SELinux 安全系统等内容的介绍，给出了基于口令的身份认证安全性分析及一次性口令的应用实例。

第 5 章为网络系统安全。首先从外在的威胁和内在的脆弱性两个方面来分析网络面临的安全问题，后续章节针对网络安全威胁以及网络协议的脆弱性，分别从网络安全设备、网络架构安全、网络安全协议、公钥基础设施和权限管理基础设施、IPv6 新一代网络安全机制等方面展开。其中，除了内容完善以外，还增加了应用实例。

第 6 章为数据库安全。首先分析了数据库安全的重要性及数据库面临的安全问题，接着给出了数据库的安全需求和安全策略，然后针对各项安全需求介绍了数据库的访问控制、完整性控制、可用性保护、可控性实现、隐私性保护等安全控制措施。另外，补充了隐私保护新技术，并给出了 4 种隐私保护技术应用分析的应用实例。最后介绍了云计算时代数据库安全控制的挑战。

第 7 章为应用系统安全。首先从应用系统面临的软件漏洞、恶意代码及软件侵权 3 个安全问题讲起，接着分别从安全软件工程、软件可信验证、软件知识产权技术保护 3 个方面有针对性地介绍应用系统安全控制技术。其中，调整了各节的顺序，补充完善了软件漏洞、安全软件工程、软件知识产权技术保护等内容，并给出了 Web 应用漏洞消减模型设计的应用实例。

第 8 章为应急响应与灾备恢复。紧紧围绕应急响应、容灾备份和恢复两大方面组织内容。本章分别完善了应急响应、容灾备份与恢复的概念，增加了应急响应过程的介绍，以及安全应急响应预案制订的应用实例，修改并补充了应急响应、容灾备份与恢复涉及的关键技术。

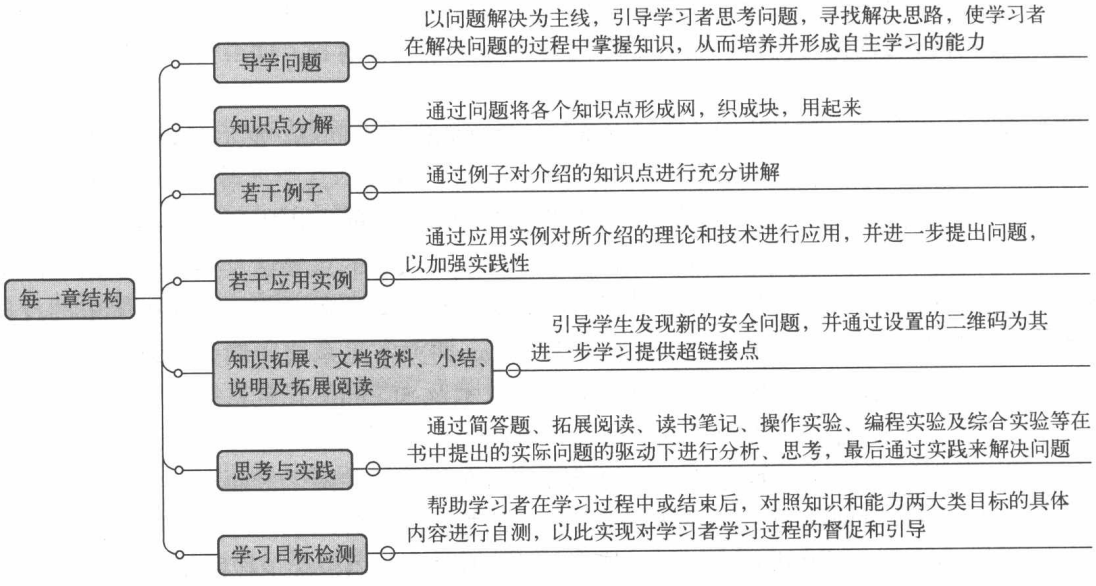
第 9 章为计算机系统安全风险评估。本章分别介绍了安全风险评估的重要性、概念、分类、基本方法和工具，重点介绍了风险评估的实施。其中，根据新的国家标准修改了安全风险评估实施阶段的各项工作。

第 10 章为计算机系统安全管理。围绕计算机系统安全管理的概念、安全管理与标准、安全管理与立法三大方面展开，补充了我国计算机安全等级保护 2.0 的相关标准、政策体系及标准体系等新内容，介绍了最新颁布的信息安全标准，结合我国新近颁布的一系列信息安全相关

法律法规，重点介绍了我国信息安全相关法律法规体系、有关恶意代码的法律惩处、有关个人信息的法律保护和管理规范，以及有关软件知识产权的法律保护等内容。

2. 编写体例创新，促进深度学习

按照建构主义的学习理论，学习者作为学习的主体在与客观环境（这里指本书内容）的交互过程中构建自己的知识结构。教学者应当引导学习者在学习和实践的过程中探索其中具有规律性的内容，将感性认识升华到理性高度，只有这样学习者才能在今后的实践中举一反三，才能有创新和发展。为此，本书第 4 版在每一章的内容组织上进行了创新，如下图所示。



本书第 4 版从正文内容的精心裁剪和组织，到课后思考与实践题的精心设计和安排，为具有高阶性、创新性和挑战度的教学提供了帮助，教师可以对学习者进行问题引导、疑难精讲、质疑点拨、检测评估，以促进学习者的深度学习和应用。

3. 实例习题丰富，注重理实结合

本书注重理论深度和广度，内容讲述深入浅出。全书通过 30 多个案例引入问题，通过数十个举例帮助读者理解并掌握相关安全原理，每一章都给出了拓展知识或二维码链接以及拓展阅读参考文献。

本书注重实践性，理论联系实际。全书通过 17 个应用实例进行实践指导，丰富了课后思考与实践题，包括简答题、知识拓展题、操作实验题、编程实验题、综合设计题和材料分析题等多种类型，共计 300 多题。

本书由陈波和于泠执笔。朱润青、朱甲领、王英东也参与并完成了部分资料的整理工作。本书在写作过程中查阅和参考了大量的文献及资料。本书的完成也要感谢机械工业出版社的郝建伟编辑一直以来对作者的指导和支持。

由于编者水平有限，书中难免有疏漏之处，恳请广大读者批评指正。为了让读者能够直接访问相关资源进行学习了解，在书中加入了大量链接，虽然已对链接地址经过认真确认，但是可能会由于网站的变化而不能访问，请予谅解。读者在阅读本书的过程中若有疑问，也欢迎与编者联系，电子邮箱是 SecLab@ 163. com。

编者

目　　录

第 1 章　计算机系统安全概论

导学问题

- 本书讨论的计算机系统是指什么？☞1.1.1 小节
- 计算机系统安全与信息安全、网络空间安全等概念有什么联系与区别？☞1.1.2 小节
- 计算机系统安全的“安全”如何理解？☞1.1.2 小节
- 安全问题产生的根源是什么？☞1.2 节
- 计算机系统安全防护的基本原则有哪些？☞1.3.1 小节
- 能否给出一个计算机系统安全防护基本体系？☞1.3.2 小节
- 计算机系统安全研究的主要内容有哪些？☞1.4 节

1.1　计算机系统安全相关概念

本节介绍计算机系统及计算机系统安全的概念。

1.1.1　计算机系统与网络空间

1. 计算机系统的定义

计算机系统（Computer System）也可称计算机信息系统（Computer Information System），按照《信息安全技术 术语》（GB/T 25069-2010）（以下简称《术语》），计算机信息系统是指“由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统”。

2017 年 6 月 1 日起实施的《中华人民共和国网络安全法》（以下简称《网络安全法》）将“网络”定义为“由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统”。

不难发现，《网络安全法》中对“网络”的界定与《术语》中对“计算机信息系统”的界定基本一致。由于计算机系统、信息、网络、网络空间这几个概念的内涵与外延有着重叠和交叉，因此依据《网络安全法》和《术语》，确定了本书研究的是网络空间环境下的计算机信息系统安全问题。

2. 网络空间环境下的计算机系统的概念

（1）“网络空间”一词的来源

为了描述人类生存的信息环境或信息空间，人们创造了 Cyberspace 一词。早在 1982 年，加拿大作家威廉·吉布森（William Gibson）在其短篇科幻小说 *Burning Chrome*（《燃烧的铬》）中创造了 Cyberspace 一词，意指由计算机创建的虚拟信息空间。后来他又在另一部小说 *Neuromancer*（《神经漫游者》）中使用这个词，将 Cyberspace 想象成一个人与计算机交融合一的广袤空间，在这个空间里，看不到高山荒野，看不见城镇乡村，只有庞大的三维信息库和各种信息

在高速流动。

Cyberspace 体现的不仅是信息的简单聚合体，也包含了信息对人类思想认知的影响。此后，随着信息技术的快速发展和互联网的广泛应用，Cyberspace 的概念不断丰富和演化。

目前，国内外对 Cyberspace 还没有统一的定义。简单地说，它是信息时代人们赖以生存的信息环境，是所有信息系统的集合。因此，通常把 Cyberspace 翻译成网络空间，突出了客观世界与数字世界交融这一重要特征。

（2）网络空间环境下计算机系统的特点

网络空间是一个与陆、海、空、天并行存在的域，涉及电磁频谱的所有领域，包括计算机、嵌入式电子设备和各类网络化基础设施等。在网络空间环境下，计算机系统涉及的软硬件组成更加广泛，结构层次更加复杂，所承载的信息更加丰富，系统与环境的交互更加密切，信息内容的传播影响更加深远。

在网络空间中，使用电子技术完成信息的产生、存储、修改、交换和利用，通过对信息的控制，实现对物理信息系统的操控，从而影响人的认知和活动。

网络空间不再只包含传统互联网所依托的各类电子设备，还包含重要的基础设施、各类应用和数据信息，人也是构成网络空间的一个重要元素。

（3）网络空间环境下计算机系统的基本组成

本书所讨论的计算机信息系统是在网络空间环境下运行的计算机信息系统，可以是一个较小的计算机信息系统，如一台计算机，也可以是复杂庞大的信息系统，如一个 Web 信息系统、云计算系统、移动智能终端系统、工业控制网络系统及物联网系统等。

网络空间环境下的计算机系统包括软硬件支撑系统、数据及信息和人。

1）计算机信息系统涉及的软硬件支撑系统的基本组成如图 1-1 所示。

<table>
<tr><td>应用业务软件</td><td rowspan="2">网络应用服务、命令等</td></tr>
<tr><td>应用平台软件</td></tr>
<tr><td>操作平台软件</td><td>网络协议等</td></tr>
<tr><td colspan="2">硬件系统（终端设备、网络设备及配套设施）</td></tr>
</table>

图 1-1　计算机信息系统涉及的软硬件支撑系统的基本组成

硬件系统包括各类终端设备（计算机、手机等）、网络设备及其他配套设施。软件系统包括操作平台软件、应用平台软件和应用业务软件。操作平台软件通常指操作系统、语言及其编译系统；应用平台软件通常指支持应用开发的软件，如数据库管理系统及其开发工具、各种应用编程和调试工具等；应用业务软件是指专为某种应用而开发的软件。

2）软硬件支撑系统只是载体，其中产生、加工、存储、传输和处理的数据和信息才是关键内涵。在计算机应用领域，数据是以数字形式表达的信息。例如，一个数据文件在计算机中的表达只是一段 0 或 1 的组合。信息则是经过加工并对客观世界产生影响的数据。

3）计算机信息系统的最终服务对象是人。人是计算机信息系统的设计者和使用者，因而研究计算机信息系统除了考虑软硬件支撑系统、数据及信息以外，还必须考虑人的因素。

1.1.2　计算机系统安全与网络空间安全

目前在我国，信息安全、网络与信息安全、网络安全、网络空间安全等术语都常使用。例如：

- 2014 年 4 月 15 日，习近平总书记在中央国家安全委员会第一次会议上提出的总体国家安全观中，国家安全体系所涵盖的 11 种安全中包括“信息安全”。
- 2015 年 7 月 1 日通过并施行的《中华人民共和国国家安全法》中，与总体国家安全观

中的“信息安全”对应的条款中采用了“网络与信息安全”的提法。

- 2016年11月7日发布的《网络安全法》中，从名称到正文，“网络安全”出现了108次，“网络空间安全”出现了一次（在第五条最后的“维护网络空间安全和秩序”这句话中）。
- 2016年12月27日，经中共中央网络安全和信息化领导小组批准，国家互联网信息办公室发布了《国家网络空间安全战略》，在标题中明确采用了“网络空间安全”，其后出现的“网络安全”只是“网络空间安全”的简称，并不等于《网络安全法》中的“网络安全”一语。

本书尝试对以上这些安全术语进行剖析和区分。

1. 网络空间安全与计算机系统安全、信息安全等概念之间的关系

在网络空间中，网络将信息的触角延伸到社会生产和生活的每一个角落。每一个网络结点、每一台计算机、每一个网络用户都可能成为信息安全的危害者和受害者。在当前这个“无网不在”的信息社会，网络成为整个社会运作的基础，由网络引发的信息安全成为了全球性、全民性的问题。

网络空间安全涉及网络空间中的电磁设备、信息通信系统、运行数据、系统应用中所存在的安全问题，既要防止、保护包括互联网、各种电信网与通信系统、各种传播系统与广电网、各种计算机系统、各类关键工业设施中的嵌入式处理器和控制器等在内的信息通信技术系统及其所承载的数据免受攻击，也要防止、应对运用或滥用这些信息通信技术系统而波及政治安全、国防安全、经济安全、文化安全、社会安全等情况的发生。

从信息论角度来看，系统是载体，信息是内涵。哪里有信息，哪里就存在信息安全问题。因此，网络空间存在更加突出的信息安全问题。网络空间安全的核心内涵仍然是信息安全。本书研究的就是网络空间（Cyberspace）中的计算机信息系统安全，即计算机系统安全。

由于计算机系统、信息、安全这几个概念的内涵与外延一直呈现不断扩大和变化的趋势，对于计算机系统安全，目前还没有一个统一的定义，为此，本小节接下来从对计算机系统安全的感性认识和安全的几大属性这两个角度，带领读者理解什么是计算机系统的“安全”。

✉ **说明：**

计算机信息系统安全、计算机系统安全、信息安全、网络空间安全等词汇中的安全在英文中通常使用的是Security，而不是Safety。这是因为，Safety侧重于对无意中造成的事故或事件进行安全保护，可以是加强人员培训、规范操作流程、完善设计等方面的安全防护工作。而Security则侧重于对人为的、有意的破坏进行防范，如部署安全设备进行防护、加强安全检测等。

不过，随着信息系统安全向网络空间安全的发展，我们既要考虑人为的、故意的针对计算机信息系统的渗透和破坏，也要考虑计算机信息系统的开发人员或使用人员无意的错误。因此，本书不对Security和Safety进行严格区分。

2. 从对安全的感性认识理解计算机系统安全

虽然迄今还没有严格的针对计算机系统安全的定义，但是当发现以下这些问题的答案时就会对此有感性认识了。

- 如果计算机的操作系统打过了补丁，那么是不是就可以说这台机器是安全的？
- 如果邮箱账户使用了强口令，那么是不是就可以说邮箱是安全的？
- 如果计算机与互联网完全断开，那么是不是就可以确保计算机安全？

从某种程度上讲，上面3个问题的答案都是“No”！因为：

- 即使操作系统及时打过补丁，但是系统中一定还有未发现的漏洞，包括 0 day 漏洞，这是系统商不知晓或是尚未发布相关补丁前就被掌握或者公开的一类漏洞；
- 即使使用强口令，但是如果用户对于口令保管不善（例如遭受欺骗而泄露，或是被偷窥），或者网站服务商管理不善，使用明文保存并泄露用户口令，都会造成强口令失效；
- 即使计算机完全与互联网断开，设备硬件仍有被窃或是遭受自然灾害的风险，计算机中的数据仍面临通过移动存储设备被泄露的威胁。

基于以上的分析，很难对安全给出一个完整的定义，但是可以从反面罗列一些不安全的情况。例如：

- 系统不及时打补丁；
- 使用弱口令，例如使用“1234”甚至是“password”作为账户的口令；
- 随意从网络下载应用程序；
- 打开不熟悉的人发来的电子邮件的附件；
- 使用不加密的无线网络。

读者还可以针对特定的应用列举更多的不安全因素，例如，针对一个电子文档分析它所面临的不安全因素，针对我们使用的 QQ、微博等社交工具分析其所面临的不安全因素。

3. 从安全的几大属性理解计算机系统安全

计算机系统的安全属性包括典型的 CIA——保密性（Confidentiality）、完整性（Integrity）和可用性（Availability），以及其他一些安全属性。

（1）保密性（Confidentiality）

保密性，也称为机密性，是指信息仅被合法的实体（如用户、进程等）访问，而不被泄露给未授权实体的特性。

这里所指的信息不但包括国家秘密，而且包括各种社会团体、企业组织的工作秘密及商业秘密，以及个人秘密和个人隐私（如浏览习惯、购物习惯等）。保密性还包括保护数据的存在性，有时存在性比数据本身更能暴露信息。特别要说明的是，对计算机的进程、中央处理器、存储设备、打印设备的使用也必须实施严格的保密措施，以免产生电磁泄漏等安全问题。

实现保密性的方法一般是物理隔离、信息加密，或是访问控制（对信息划分密级并为用户分配访问权限，系统根据用户的身份权限控制其对不同密级信息的访问）等。

（2）完整性（Integrity）

完整性是指信息在存储、传输或处理等过程中不被未授权、未预期或无意地篡改、销毁等破坏的特性。

不仅要考虑数据的完整性，还要考虑系统的完整性，即保证系统以无害的方式按照预定的功能运行，不被有意的或者意外的非法操作所破坏。

实现完整性的方法一般有预防和检测两种机制。预防机制通过阻止任何未经授权的行为，来确保数据的完整性，如加密、访问控制。检测机制并不试图阻止完整性的破坏，而是通过分析数据本身或是用户、系统的行为来发现数据的完整性是否遭受破坏，如数字签名、哈希（Hash）值计算等。

（3）可用性（Availability）

可用性是指信息、信息系统资源和系统服务可被合法实体访问并按要求使用的特性。

对信息资源和系统服务的拒绝服务攻击就属于对可用性的破坏。

实现可用性，可以采取应急响应、备份与灾难恢复等措施。