<<信息安全技术概论>>

图书基本信息

书名：<<信息安全技术概论>>

13位ISBN编号：9787121085789

10位ISBN编号：712108578X

出版时间：2009-4

出版时间：电子工业出版社

作者：冯登国，赵险峰　编著

页数：240

前言

在古往今来的政治军事斗争、商业竞争等活动中，人们常常希望他人不能获知或篡改某些信息，也常常需要查验信息的可信性，“信息安全”一词就是指实现以上目标的能力或状态。
随着存储、处理和传输信息手段的变化和进步，信息安全面临更大挑战，它的内涵也不断延伸。
当前，信息安全可被理解为信息系统抵御意外事件或恶意行为的能力，这些事件和行为危及所存储、处理或传输的数据，或者危及由这些系统所提供的服务的可用性、机密性、完整性、非否认性、真实性和可控性。
其中，可用性指能够保障数据和服务的正常使用；机密性指能够确保数据的传输和存储不受未授权的浏览，甚至不暴露保密通信的事实；完整性指能够确保数据是完整的，在被篡改的情况下能够发现篡改；非否认性指能够保证信息系统的操作者或信息的处理者不能否认其行为或处理结果；真实性指能够确保人、进程或系统等身份或信息、信息来源的真实；可控性指能够保证掌握和控制信息与信息系统的基本情况，可对它们的使用实施授权、审计、责任认定、传播源追踪和监管等控制。
顾名思义，信息安全技术是指保障信息安全的技术，它主要包括对信息的伪装、验证和对信息系统的保护等方面。
信息安全技术由来已久，相关内容较多地出现在了古代东、西方的文字记载中，但它仅在第二次世界大战以后才获得了长足的发展，由主要依靠经验、技艺逐步转变为主要依靠科学，因此，信息安全是一个古老而又年轻的科学技术领域。
当前，随着社会信息化程度的提高，许多国家和地区采取了有力的措施推进信息安全技术与相关技术的发展，信息安全的研究与开发显得更加活跃，人们关心的信息安全问题已经从早期的机密性扩大到以上全部6个属性，形成了较为复杂的信息安全技术体系。
信息安全技术主要包括以下5类：核心基础安全技术（包括密码技术、信息隐藏技术等）、安全基础设施技术（包括标识与认证技术、授权与访问控制技术等）、基础设施安全技术（包括主机系统安全技术、网络系统安全技术等）、应用安全技术（包括网络与系统攻击技术、网络与系统安全防护与应急响应技术、安全审计与责任认定技术、恶意代码检测与防范技术、内容安全技术等）、支撑安全技术（包括信息安全测评技术、信息安全管理技术等）。
由于信息安全面临的问题较多，在方法上涉及数学、物理、微电子、通信、计算机等众多领域，有着覆盖面广的技术体系和丰富的科学内涵，因此要全面阐述、把握它并非易事。
尤其是，随着信息技术的发展，近十年来信息安全技术体系发生了一些较显著的变化，因此，它的概貌也有必要得到新的描述。
为了帮助在校学生、相关研究人员和感兴趣的读者全面了解信息安全技术的基本原理、方法及各项技术之间的关系，本书概括地介绍了主要的信息安全技术，依次为密码技术、标识与认证技术、授权与访问控制技术、信息隐藏技术、网络与系统攻击技术、网络与系统安全防护与应急响应技术、安全审计与责任认定技术、主机系统安全技术、网络系统安全技术、恶意代码检测与防范技术、内容安全技术、信息安全测评技术、信息安全管理技术，所介绍的内容涉及这些技术的基本术语与概念、发展历史与发展趋势、面对的威胁与安全需求、采取的基本安全模型与策略、典型的安全体系结构和安全机制、基本实现方法等方面。
本书每章配有论述与思考题，以供巩固之用。
本书是作者在长期从事科研与教学的基础上编写的。
本书的编写得到了国家自然科学基金项目（编号：60673083、60573049）的支持。
在一些内容的讨论和数据、参考资料的提供方面，编写工作也得到了信息安全国家重点实验室相关科研、教学人员和研究生的帮助，他们包括吴文玲研究员、连一峰副研究员、苏璞睿副研究员、张立武高工、张敏高工和博士生夏冰冰、邓艺、王蕊等，作者在此一并向他们表示感谢。
作者感谢本书的审核专家蔡吉人院士提出的建设性和指导性意见，还要感谢电子工业出版社的刘宪兰编辑在本书成稿过程中给予的各种支持和帮助。
作者希望本书的出版能为信息安全技术与观念在我国的普及尽微薄之力！

<<信息安全技术概论>>

内容概要

本书概括地介绍了主要的信息安全技术，包括密码、标识与认证、授权与访问控制、信息隐藏、网络与系统攻击、网络与系统安全防护与应急响应、安全审计与责任认定、主机系统安全、网络系统安全、恶意代码检测与防范、内容安全、信息安全测评、信息安全管理等技术，所介绍的内容涉及这些信息安全技术的基本术语与概念、发展历史与发展趋势、面对的威胁与安全需求、采取的基本安全模型与策略、典型的安全体系结构和安全机制、基本实现方法等方面。
本书有助于读者全面了解信息安全技术的基本原理、方法及各项技术之间的关系，适合作为高等学校信息安全专业本科生和相关专业的高年级本科生或研究生的教材，也适合供相关科研人员和对信息安全技术感兴趣的读者阅读。

<<信息安全技术概论>>

书籍目录

章节摘录

插图：第1章 绪论1.1 什么是信息安全信息安全问题在人类社会发展中从古至今都存在。
在政治军事斗争、商业竞争甚至个人隐私保护等活动中，人们常常希望他人不能获知或篡改某些信息，并且也常常需要查验所获得信息的可信性。
普通意义上的信息安全是指实现以上目标的能力或状态。
例如，人们在工作中常提到：系统的信息安全怎样、有没有信息安全保障等。
信息安全自古以来一直受到人们的重视。
我国春秋时代的军事家孙武（公元前535年-不详）在《孙子兵法》中写道：“能而示之不能，用而示之不用，近而示之远，远而示之近。
”这显示了孙武对军事信息保密的重视。
古罗马统治者Caesar（公元前100年-公元前44年）曾使用字符替换的方法传递情报，例如，将a、b、C等分别用F、G、H等来表示，这反映了他对通信安全的重视。
随着人类存储、处理和传输信息方式的变化和进步，信息安全的内涵在不断延伸。
当前，在信息技术获得迅猛发展和广泛应用的情况下，信息安全可被理解为信息系统抵御意外事件或恶意行为的能力，这些事件和行为将危及所存储、处理或传输的数据或由这些系统所提供的服务的可用性、机密性、完整性、非否认性、真实性和可控性。
以上这6个属性刻画了信息安全的基本特征和需求，被普遍认为是信息安全的基本属性，其具体含义如下。
（1）可用性（Availability）。
即使在突发事件下，依然能够保障数据和服务的正常使用，如网络攻击、计算机病毒感染、系统崩溃、战争破坏、自然灾害等。
（2）机密性（Confidentiality）。
能够确保敏感或机密数据的传输和存储不遭受未授权的浏览，甚至可以做到不暴露保密通信的事实。
（3）完整性（Integrity）。
能够保障被传输、接收或存储的数据是完整的和未被篡改的，在被篡改的情况下能够发现篡改的事实或者篡改的位置。
（4）非否认性（Non．repudiation）。
能够保证信息系统的操作者或信息的处理者不能否认其行为或者处理结果，这可以防止参与某次操作或通信的一方事后否认该事件曾发生过。
（5）真实性（Authenticity）。
真实性也称可认证性，能够确保实体（如人、进程或系统）身份或信息、信息来源的真实性。
（6）可控性（Controllability）。
能够保证掌握和控制信息与信息系统的基本情况，可对信息和信息系统的使用实施可靠的授权、审计、责任认定、传播源追踪和监管等控制。

<<信息安全技术概论>>

版权说明