信息系统安全的理论与实践研究

XINXI XITONG ANQUAN DE
LILUN YU SHIJIAN YANJIU

◎ 韦鹏程　韦玉轩　邹晓兵　著

电子科技大学出版社

信息系统安全的理论与实践研究

韦鹏程　韦玉轩　邹晓兵　著

电子科技大学出版社
University of Electronic Science and Technology of China Press

图书在版编目(CIP)数据

信息系统安全的理论与实践研究/韦鹏程，韦玉轩，邹晓兵著.
-- 成都：电子科技大学出版社，2017.7
ISBN 978-7-5647-4866-1

Ⅰ.①信… Ⅱ.①韦…②韦…③邹… Ⅲ.①信息系统-安全技术-研究 Ⅳ.①TP309

中国版本图书馆CIP数据核字(2017)第182241号

信息系统安全的理论与实践研究

韦鹏程 韦玉轩 邹晓兵 著

策划编辑 李述娜

责任编辑 谭炜麟

出版发行 电子科技大学出版社

成都市一环路东一段159号电子信息产业大厦九楼 邮编 610051

主 页 www.uestcp.com.cn

服务电话 028-83203399

邮购电话 028-83201495

印 刷 北京一鑫印务有限责任公司

成品尺寸 170mm × 240mm

印 张 20.25

字 数 415千字

版 次 2017年12月第一版

印 次 2017年12月第一次印刷

书 号 ISBN 978-7-5647-4866-1

定 价 70.00元

前　言

随着计算机技术与网络通信技术的飞速发展，计算机网络信息应用已经渗透到社会经历领域的各个方面。计算机网络信息技术是现在信息科学与技术的重要组成部分，也是计算机管理信息系统的核心；计算机网络信息安全管理即使信息化推进的基础保障，也是信息系统正常运行的关键环节。计算机和网络信息系统不断受到侵害，侵害形式日益多样化，侵害手段和技术日趋现金和复杂化，已经严重威胁到网络和信息的安全。信息安全是指网络系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露。网络信息系统连续可靠正常运行，网络服务不中断。

正如人是现实社会生活中的行为单元一样，主机是信息网络空间中的工作单元。为了维护现实社会生活的安定与和谐，公安机关采取了对犯罪分子进行严厉打击的措施，为了确保信息网络空间的安全与可信，有必要对主机系统的安全问题准确地把握。

信息安全事关国家安全，因为信息化已经渗透到人类社会的各个层面。系统的安全在信息安全中举足轻重，因为所有的软件最终都必须落实到具体的主机系统上运行。解剖信息网络空间中的安全问题，就能清楚地看到主机系统安全是其中不可或缺的成分，而解剖主机系统的安全问题，就会发现它自身的内容也是丰富多彩的。

而且随着当下移动信息网络接入带宽的提升以及移动终端软硬件的快速更新，伴随着大数据、电子商务等重要计算技术的发展，移动互联网成为当前学术界和创业界关注的热点。由于移动设备具有便携性，移动互联网真正使得“任何地方、任何时间、任何人”享受网络服务成为可能。用户在家里、地铁、机场等随处尽可享受社交网络、电子商务、手机电子、移动支付等各种移动互联网应用服务。随着移动互联网的发展，特别是电子商务、手机支付应用的普及，移动互联网安全成为移动互联网健康发展的重要保障。保证移动互联网安全设计众多具体细节问题，如通

信安全、传输安全、传统的加密方法在资源首先的移动终端商的解决方案、终端安全、终端应用安全等问题。

本书结合现代计算机技术，参考大量中外文献，研究互联网信息安全系统管理发展趋势。从密码学的角度对信息系统安全进行探究，并根据黑客入侵、网络病毒破坏、防火墙安全来研究网络信息系统安全的技术，并结合操作系统及数据库等来探究其安全机制。

本专著由重庆第二师范学院韦鹏程教授，广西建设职业技术学院韦玉轩副教授，重庆第二师范学院邹晓兵博士、李莉博士和石熙博等五位教师完成，并得到重庆市交互式电子教育工程技术研究中心、重庆第二师范学院交互式电子产品协同创新中心支持和重庆第二师范学院计算机科学与技术重点学科项目，在此表示感谢！

目　录

第一章 信息安全

随着社会信息化程度的提高，信息安全面临诸多挑战，许多国家和地区采取了有力措施，推进信息安全技术的发展，活跃了当前信息安全的研究与开发。

第一节 信息安全的概述

信息安全问题古已有之。最初，人们仅以实物或特殊符号传递机密信息，后来出现了一些朴素的信息伪装方法。随着人类存储、处理和传输信息手段的进步，信息安全的内涵也不断延伸在政治军事斗争、商业竞争和公民个人隐私保护等活动中，往往需要保护己方信息不被他人获知或篡改，在取得信息时，往往也需要确认该信息是否可信。在一般意义上，信息安全是指实现以上目标的能力或状态在信息技术应用的背景下，信息安全可理解为信息系统抵御意外事件或恶意行为的能力。

一、信息安全属性

由于信息安全受到了政府和企业的普遍重视，众多国内外的标准化组织都把信息安全纳入其标准体系中但在不同标准体系，所给出的信息安全具体定义却不尽相同。例如，美国国家安全系统委员会（Committeeon National Security Systems，CNSS）将信息安全定义为：保护信息及其关键要素，包括使用、存储以及传输信息的系统和硬件。CNSS 将机密性、完整性和可用性作为信息安全概念的基础。《信息安全管理体系原理与术语》将信息安全定义为：保护、维持信息的机密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。

总结关于信息安全的各种定义，一个信息系统的基本信息安全需求，可以由机密性、完整性、可用性、不可否认性、可认证性和可控性等基本属性来刻画，它们的具体含义如下。

（一）机密性（Confidentiality）

确保敏感或机密数据在存储、使用、传输过程中不会泄露给非授权用户或实体的特性，甚至可以做到不暴露保密通信的事实，具有敏感性的秘密信息，只有得到许可才能够获得该信息，防止信息的非授权访问或泄露。

（二）完整性（Integrity）

确保信息在存储、传输或接收的过程中，其原有的内容、形式与流向，既不能被未经授权的第三方所篡改，也不会被授权用户进行不恰当的修改。而在被篡改的情况下，应能够检测出其被篡改的事实或者篡改的位置。

（三）可用性（Availability）

确保信息可被授权者访问并按需求使用的特性，保证合法用户对信息和资源的使用不会被不合理地拒绝。即使在突发事件下，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，依然能够保障数据和服务的正常使用。

（四）不可否认性（Non-repudiation）

能够保证信息系统的操作者或信息的处理者无法否认其行为或者处理结果，防止参与某次操作或通信的一方事后否认该事件的发生，为出现的信息安全事件提供调查的依据。

（五）可认证性（Authenticity）

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。

（六）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。

二、信息安全威胁

信息系统安全威胁是指，对信息系统的组成要素及功能造成某种损害的潜在可能信息系统安全所面临的威胁来自多方面，并且随着时间的变化而变化，目前还没有一个统一的方法对各种威胁进行准确的分类。下面按照威胁来源、威胁实施手段，以及按通信中的信息流向对信息系统所面临的常见安全威胁进行分类介绍。

（一）按照威胁来源分

信息系统的威胁源可以分为系统内部和外部。据此，可将其所面临的安全威胁分为内部威胁和外部威胁。根据是否有人为干预，进一步地可将威胁分为自然威胁和人为威胁。自然威胁是指来自于各种自然灾害、恶劣的场地环境、设备老化等。这些无目的的事件，有时会直接威胁系统运行和信息安全，影响信息的存储媒体。对于这些灾害，虽然不能阻止其发生，但是可以通过技术或管理手段，避免或降低灾害带来的损失。根据操作人员是否存在主观故意，人为威胁可以分为无意威胁和恶意攻击。

1. 无意威胁

此类威胁没有明显的恶意企图，其主要肇因是系统内部人员操作不当或失误。

例如，操作员安全设置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享等，都会对信息系统安全带来威胁，此类威胁在信息系统的整个生命周期中始终存在，会破坏信息系统的安全性。有关安全专家经过长期的调查得出结论：无论是私人机构，还是公共机构，大约65%的损失是由于无意的错误或疏忽所造成的。

2.恶意攻击

此类威胁是利用信息系统暴露的弱点，对其实施攻击，使得信息系统的机密性、完整性、可用性等安全属性受到损害，是有目的的人为恶意破坏，可分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地对信息系统实施破坏，如对信息进行修改、删除、伪造、添加、重放、乱序、冒充，以及制造病毒等。而被动攻击是指在不干扰网络信息系统正常工作的情况下，进行窃听、截获、窃取、破译和业务流量分析等。由于恶意攻击有明显的企图，其危害性相当大，给政治、经济和文化等领域的活动，以及知识产权、个人信息的保护，甚至国家安全都带来巨大的威胁。

（二）按照威胁实施手段分

根据威胁实施的手段或方法，常用的威胁可以分为以下7种。

1.信息泄露

指系统的敏感数据被未授权者获取，从而破坏了信息的机密性。信息泄露的主要途径有：

（1）窃取：有两种情形，一是盗用存储设备，二是利用电磁辐射或搭接线路等方式窃听传输中的信息。

（2）通过构建隐蔽的泄密信道，向未授权者泄露信息。例如，在传输文件时，对文件名进行特殊编码以传递秘密信息，从而使正常的文件传输信道成为隐蔽的泄密信道。

（3）通过分析通信行为，获取敏感信息。未授权者利用特定的工具捕获网络中的数据流量、流向、通信频带和数据长度等数据并进行分析，从中获取敏感信息。

2.系统入侵

入侵是指未经授权就获得系统的访问权限或特权，对系统进行非正常访问，或擅自扩大访问权限非授权访问主要有如下4种。

（1）旁路控制：攻击者利用系统漏洞绕过系统的访问控制而渗入系统内部。

（2）假冒：攻击者通过出示伪造的凭证骗取系统的信任，非法取得系统访问权限或得到额外的特权。

（3）口令破解：利用专门的工具穷举或猜测用户口令。

（4）合法用户的越权访问：合法用户进入系统后，擅自扩大访问权限。

3. 传播恶意代码

恶意代码是一些对系统具有现实或潜在危害的代码。它们或独立存在，或依附于其他程序恶意代码有可能大量消耗系统资源，或者进行删除和修改等破坏性操作，或者执行窃取敏感数据的任务，

4. 拒绝服务

拒绝服务（DoS）指系统可用性因服务中断而遭到破坏。DoS 攻击常常通过使用户进程消耗过多的系统资源，造成系统阻塞或瘫痪。

5. 系统扫描

利用特定的工具向目标系统发送特制的数据包，并通过分析其响应，以了解目标网络或主机的特征，为后续攻击做准备。

6. 信息重放

攻击者先记录系统中的合法信息，然后在适当的时候重放，使系统难辨真伪，达到混淆视听、扰乱系统的目的。

7. 抵赖

指通信一方出于各种目的，而实施的以下行为：发送方事后否认自己曾经发送过某些消息；发送方事后否认自己曾经发送过某些消息的内容；接收方事后否认自己曾经收到过某些消息；接收方事后否认自己曾经收到过某些消息的内容。

（三）按照对系统信息流的影响分

按照安全威胁对信息系统通信信息流的影响，可将威胁分为中断威胁、截获威胁、篡改威胁和伪造威胁。

1. 中断威胁

在正常情况下，信息系统的正常信息流向如图 1-1 所示。当发生中断威胁后，信息流受到阻断，结果如图 1-2 所示。中断威胁会破坏信息系统的可用性。最常见的中断威胁是造成信息系统的拒绝服务，即信息系统或信息资源的利用价值或服务能力下降或丧失。

图 1-1　正常的信息流向

图 1-2 中断威胁

2. 截获威胁

如图 1-3 所示，截获威胁是指一个非授权实体介入了系统，使得信息在传输过程中被拦截监听。这里，非授权实体可以是人、程序或计算机。截获攻击可以破坏信息系统的机密性。

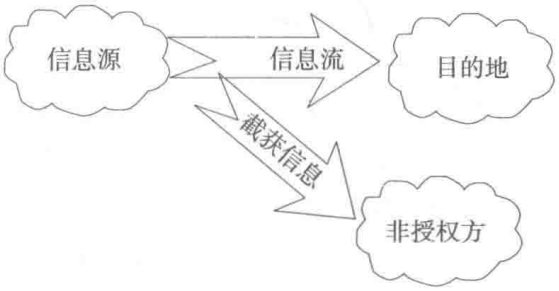

图 1-3 截获威胁

3. 篡改威胁

如图 1-4 所示，篡改威胁是指一个非授权实体取得了对系统信息流的控制权，可以未经授权对其进行修改、删除和重放等操作，使信息的完整性受到破坏。此类攻击还包括对存储数据和程序的篡改，使之不能正确解析或执行

图 1-4 篡改威胁

4. 伪造威胁

如图 1-5 所示，伪造威胁是指一个非授权实体将伪造的信息植入系统，从而破坏了系统信息的真实性，例如，向系统的合法用户传送虚假信息。

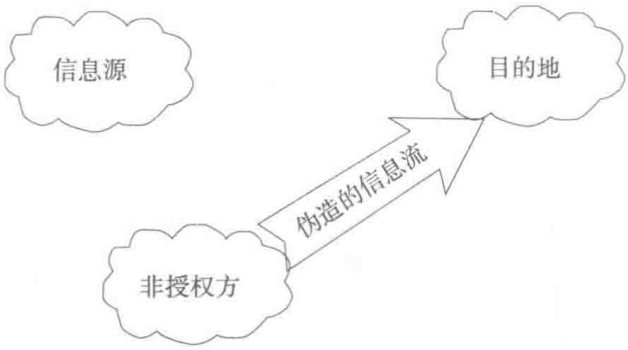

图 1-5　伪造威胁

三、信息安全发展历程

信息安全是一个古老而又年轻的科学技术领域，在不同历史阶段，受应用需求的驱动，其内涵也逐步丰富完善特别是在第二次世界大战以后，它获得了长足发展，由主要依靠经验、技艺逐步转变为主要依靠科学。在短短的几十年间，其内涵由通信保密演变为计算机安全，进而发展为信息安全，直至目前的信息保障。

（一）通信保密阶段（COMSEC）

20 世纪 60 年代之前，人们对信息安全的关注，主要集中在通信的机密性，这个发展时期可以归结为通信保密阶段。在这个阶段，信息安全的主要关注者是军方和政府机构。信息安全所要解决的问题，主要是如何在远程通信中，防止信息被非授权方截获，以及确保通信的真实性而确保信息安全的主要手段，则是信息加密和信息隐藏。例如，在我国北宋年间的《武经总要》中，记载了北宋军队对军令的伪装方法：先将全部 40 条军令编号，并汇成码本，以 40 字的诗对应位置上的文字代表相应编号；在通信中，代表某编号的文字被隐藏在一个普通文件中，但接收方知道它的位置，这样就可以通过查找该字在 40 字诗中的位置获得编号，再通过码本获得军令，按现在的观点，它综合了基于密码本的加密和基于文本的信息隐藏。

自 19 世纪 40 年代发明电报后，安全通信主要面向保护电文的机密性，密码技术成为获得机密性的核心技术。在两次世界大战中，各发达国家均研制了自己的密码算法和密码机。例如，在第二次世界大战中，德国发明了 ENIGMA 密码机、日本发明了 PURPLE 密码机。但当时的密码技术没有摆脱主要依靠经验的设计方法，

并且由于在技术上没有安全的密钥或码本分发方法，在两次世界大战中有大量的密码通信被破解。以上密码被普遍称为古典密码。

1949 年，Shannon 提出了著名的 Shannon 保密通信模型，这是通信保密阶段的时代标志。Shannon 的保密通信模型，明确了密码设计者需要考虑的问题，并用信息论阐述了保密通信的原则，为对称密码学奠定了理论基础，将密码学的研究纳入了科学的轨道。

（二）计算机安全阶段（COMPUSEC）

计算机安全阶段跨越了 20 世纪 60 年代中期至 80 年代。计算机的出现深刻改变了人类处理和使用信息的方法，也使信息安全的内涵扩展到了计算机和信息系统的安全。20 世纪 60 年代出现了多用户操作系统，为了解决计算机资源和信息的安全共享问题，人们对信息安全的关注扩大到机密性、访问控制与认证，并逐渐注意到保障可用性。1965—1969 年，美国军方和科研机构组织开展了有关操作系统安全的研究。1969 年，Lanlpson 提出了主体（Subject）、客体（Object）和访问矩阵（Access Matrix）等概念，第一次用形式化的方法对访问控制问题做了抽象；1972 年，Anderson 报告提出了引用监控器、引用验证机制、安全内核和安全建模等重要思想，指出要开发安全系统，首先必须建立系统的安全模型，完成安全系统建模之后，其次再进行安全内核的设计与实现；1973 年，Lampsori 提出了隐蔽通道的概念，他发现两个被限制通信的实体之间如果共享某种资源，那么它们就可以利用隐蔽通道传递信息；同年，Bell 和 LaPadula 提出了第一个经过严格数学证明的安全模型，即 BLP 模型。

在这一阶段，为了评价计算机系统的安全性，美国、加拿大和欧洲主要国家各自推出了自己的信息系统安全评价标准 1985 年，美国国防部推出了《可信计算机系统评价准则》（TCSEC），该标准是世界上第一部关于计算机系统的安全评测标准，是信息安全领域中的重要创举，为后来英、法、德、荷四国联合提出的同时涵盖保密性、完整性和可用性需求的《信息技术安全评价准则》（ITSEC）打下了基础

在这一阶段，密码学领域也取得了重要成果。1976 年，Diffie 和 Heilman 发表了《密码学的新方向》一文，指出在通信双方之间不直接传输加密密钥的保密通信是可能的，并提出了公钥加密的设想；1977 年，美国国家标准与技术研究所（N[ST）首次通过公开征集的方法，制定了当时应用中急需的“数据加密标准（DES）”，推动了分组密码的发展。这两个事件标志着现代密码学的诞生。1978 年，Rivest、Shamir 与 Adleman 设计了著名的 RSA 公钥密码算法，实现了 Diffie 和 Heilman 提出的公钥加密思想，使数字签名和基于公钥的认证成为可能。

（三）信息安全阶段（INFOSEC）

20 世纪 80 年代中期以后，随着信息技术应用越来越广泛和网络的普及，学术

界、产业界、政府和军事部门等对信息和信息系统安全越来越重视。人们除了要求信息在存储、处理和传输过程中不被非法访问或者篡改，确保合法用户获得服务并限制非授权用户使用服务外，还要求能够检测、记录和抵御攻击。在这一时期，密码学、安全协议、计算机安全、安全评估和网络安全技术得到了较大发展，尤其是互联网的应用和发展大大促进了信息安全技术的发展与应用。因此，信息安全的这一发展阶段也可以称为网络安全阶段。

在这一时期，不但学术界提出了很多新观点和新方法，如椭圆曲线密码（ECC）、密钥托管和盲签名等，标准化组织与产业界也制定了大量的算法标准和实用协议，如数字签名标准（DSS）、IP 安全协议（IPSec）等。此外，安全多方计算、形式化分析、零知识证明、可证明安全性等均取得了进展，一些理论成果也逐渐能够得到应用，在安全评测方面，20 世纪 90 年代中期，加拿大、法国、德国、荷兰、英国和美国提出了《信息技术安全性评估通用准则》（CC 标准）。

在这一时期，网络攻击事件逐渐增多，传统的安全保密措施难以抵御计算机黑客入侵及有组织的网络攻击，学术界和产业界先后提出了防火墙、入侵检测系统和虚拟专用网等网络安全防护技术。1989 年，美国国防部资助卡耐基梅隆大学建立了世界上第一个计算机应急小组及协调中心（CERT/CC，Computer Emergency Response Team/Coorflinalion Center），标志着信息安全从被动防护阶段过渡到主动防护阶段。人们除了要求信息在存储、处理和传输过程中不被非法访问或者篡改，确保合法用户获得服务并限制非授权用户使用服务外，还要求能够检测、记录和抵御攻击。于是除了信息的机密性、完整性和可用性之外，人们对信息的安全性提出了可控性、可认证性和抗抵赖等新的要求

（四）信息保障阶段（A）

20 世纪 90 年代中期以来，随着信息安全越来越受到各国的高度重视，以及信息技术本身的发展，人们更加关注信息安全的整体发展及在新型应用下的安全问题人们也开始深刻认识到，安全是建立在过程的基础之上的，信息安全的发展也越来越多地与国家战略结合在一起在此背景下，信息安全从单纯信息安全防护向综合信息保障（IA，Information Assurance）的方向发展，1995 年，美国国防部提出了“保护—检测—响应”的动态模型，即 PDR（Protection，Detection，Reaction）模型；1998 年 10 月，美国国家安全局（NSA）颁布了信息保障技术框架（IATF，lnformalio IAssuranceTechnical Framework），它从信息保护过程的角度，提出信息保障应包括保护、检测、反应和恢复等环节保护是指利用数据加密、用户认证，访问控制等技术保证数据的各种属性；检测是指利用各种技术手段，检测并记录危及信息安全的各种攻击行为，并提供事后审计和查询功能；反应是指在检测出攻击行

为之后，在攻击过程中或者攻击结束后采取必要的策略，避免攻击再次发生，或者减少攻击行为带来的破坏；恢复是指在攻击对信息或信息系统已经造成破坏后，采用数据恢复、应用恢复等方式，尽量使信息或信息系统恢复到被破坏前的状态。在信息保障框架下，保护、检测、反应和恢复是一个统一的过程，它不再过分强调“严防死守”，而是要保证网络在遭受攻击的情况下，能够及早地识别、检测出这些攻击，将可能造成的损失降到最低程度，并保证信息系统基本业务的连续性。信息保障的策略是深层防护、多级配置，使得在深层防护架构内，各种安全设施和手段互相支持，达到整体的信息安全效果。

在这一阶段，信息安全的相对性、动态性、系统性等特征引起人们的注意，追求适度风险的信息安全成为共识安全不再是单纯以功能或者机制技术的强度作为评价指标，而是结合了不同主体的应用环境和应用目标的需要，进行合理的计划、组织和实施：此外，人们认识到，不但要从技术上，而且还要从管理上建立一个包含人的因素在内的信息安全管理体系，使得信息安全管理成为时代的需要。

第二节 信息安全技术体系分析

与信息安全的发展历程一样，信息安全技术在不同阶段也表现出不同的特点。在通信保密阶段，针对数据通信的保密性需求，人们对密码学理论和技术的研究及其应用逐渐成熟起来。随着计算机和网络技术的急剧发展，信息安全阶段的技术要求集中表现在 IS07498-2 标准中陈述的各种安全机制上，这些安全机制的共同特点就是对信息系统的保密性、完整性和可用性进行静态保护。发展到了信息保障阶段之后，信息安全技术已经不再是以单一的防护为主，而是包括了防护、检测、响应和恢复几个关键环节的动态发展的完整体系。从信息安全防护层面看，当前主要信息安全技术有以下几类。

一、安全基础技术

（一）密码技术

密码技术主要包括密码算法和密码协议的设计与分析技术密码算法包括分组密码、序列密码、公钥密码、杂凑函数、数字签名等，它们在不同的场合分别用于提供机密性、完整性、真实性、可控性和不可否认性，是构建安全信息系统的基本要素。密码协议是在消息处理环节采用了密码算法的协议，它们运行在计算机系统、网络或分布式系统中，为安全需求方提供安全的交互操作。密码分析技术指在获得

一些技术或资源的条件下破解密码算法或密码协议的技术。

（二）标识与认证技术

从信息安全的角度看，需要对信息系统中出现的实体进行标识和身份鉴别，这类技术称为标识与认证技术。所谓标识是指实体的表示，信息系统从标识可以对应到一个实体例如，用户名、进程名、主机名等，都是计算机系统中常见的标识，没有标识就难以对系统进行安全管理。认证技术就是鉴别实体身份的技术，主要包括口令技术、生物认证技术和公钥认证技术等，还包括对数据起源的验证。随着电子商务和电子政务等分布式安全系统的出现，基于公钥密码技术的公钥基础设施（Public Key Infrastruclure，PKI）技术在经济和社会生活中的作用越来越大。

（三）授权与访问控制技术

为了使得合法用户正常使用信息系统，需要给已通过认证的用户授予相应的操作权限，这个过程被称为授权。在信息系统中，可授予的权限包括读/写文件、运行程序和访问网络等，实施和管理这些权限的技术称为授权技术。访问控制技术和授权管理基础设施（Privilege Management Infraslruclure，PMI）技术是两种常用的授权技术，访问控制在操作系统、数据库和应用系统的安全管理中具有重要作用，PMI 是支持授权服务的安全基础设施，可为访问控制提供授权管理支持。从应用目的上看，网络防护中的防火墙技术也有访问控制的功能，但由于实现方法与普通的访问控制有较大不同，一般将防火墙技术归入网络防护技术。

（四）安全审计与责任认定技术

为抵制网络攻击、电子犯罪和数字版权侵权，安全管理或执法部门需要相应的事件调查方法与取证手段，这种技术统称为安全审计与责任认定技术。审计系统普遍存在于计算机和网络系统中，它们按照安全策略记录系统出现的各类审计事件，主要包括用户登录、特定操作、系统异常等与系统安全相关的事件。安全审计记录有助于调查与追踪系统中发生的安全事件，为诉讼电子犯罪提供线索和证据。随着计算机和网络技术的发展，数字版权侵权的现象在全球都比较严重，需要对这些散布在系统外的事件进行监管，当前，已经可以将代表数字内容购买者或使用者的数字指纹和可追踪码嵌入内容中，在发现版权侵权后进行盗版调查和追踪。

二、安全支撑技术

（一）信息安全测评技术

信息安全测评是指对信息安全产品或信息系统的安全性等进行验证、测试、评价和定级，以规范它们的安全特性，而信息安全测评技术就是能够系统、客观地验证、测试和评估信息安全产品和信息系统安全性质和程度的技术。虽然密码和信息