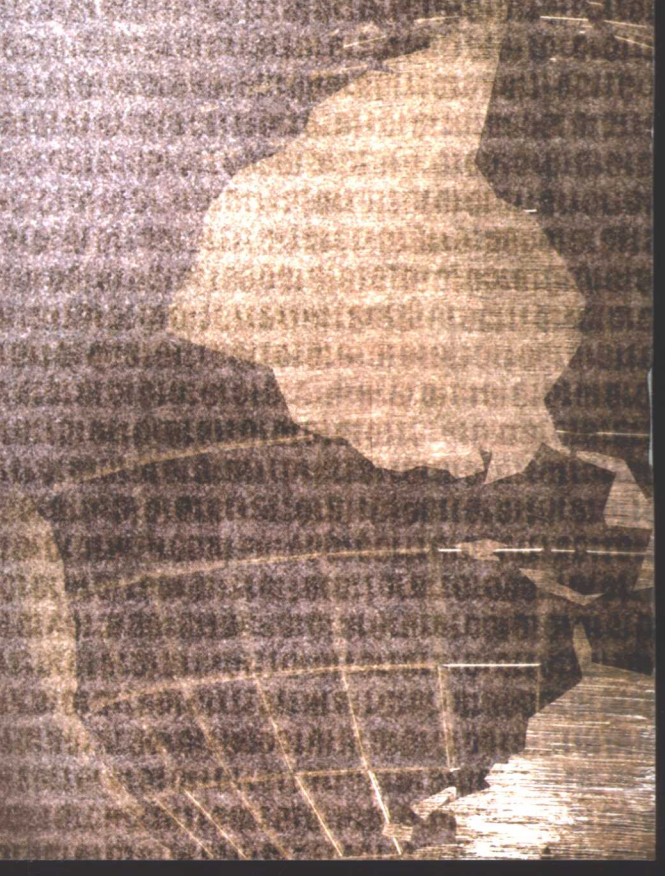
国家科学技术学术著作出版基金

信息安全工程导论

沈昌祥 编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信息安全工程导论

沈昌祥　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书介绍并分析了信息安全工程方法，共分 10 章。第 1 章简介了信息安全保障的基本概念和信息安全工程方法的发展；第 2～4 章说明了系统工程过程与信息系统安全工程（ISSE）；第 5～7 章分析了包括 SSE-CMM 体系结构在内的 SSE-CMM 方法学以及 SSE-CMM 的域维和能力维；第 8 章分析了 SSE-CMM 的完备性；第 9 章的主题是信息安全工程与我国计算机信息系统安全等级保护的关系；第 10 章将信息安全工程方法置于 ISO/IEC 15443《IT 安全保证框架》的背景中进行了讨论。

本书可以作为信息安全专业研究生的教学用书和信息安全专业技术培训用书，也可供信息安全技术人员、管理人员和研究者阅读。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

信息安全工程导论/沈昌祥编著. —北京：电子工业出版社，2003.7
ISBN 7-5053-8826-6

Ⅰ. 信… Ⅱ. 沈… Ⅲ. 信息系统—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2003）第 048239 号

责任编辑：宋 漪　　特约编辑：叶 林
印　　刷：北京市增富印刷有限责任公司
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：18　字数：467.3 千字
版　　次：2003 年 7 月第 1 版　2003 年 7 月第 1 次印刷
印　　数：4 000 册　　定价：36.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。
联系电话：（010）68279077

前言

爱因斯坦说过："我们创造的世界是我们的思维水平所能达到的结果，因此也在很大程度上制造了在创造它们的同一水平上我们所不能解决的问题。"

第三次生产力革命——信息革命以来，人类逐步跨入数字化生存的新境界。但这个新的生存境界是不是正在按其创造者——人类的意志所存在和发展呢？伟大的智者已经给出了答案。

因此，当面对严峻的信息安全挑战时，我们首先要解决的是态度问题。因噎废食和盲目乐观都是不可取的，而宣扬全面、彻底的解决方案，期望一劳永逸地解决信息安全问题的做法也有违于客观规律。信息安全问题是信息革命与生俱来的伴随物。在信息化进程中，只要求发展，就必然会面临信息安全问题。

但是我们正在化被动为主动，在与真理无限接近的过程之中，我们始终在努力寻求对信息安全本质及其规律的掌握。即使不能在一时的知识层面上解决全部的问题，我们仍然期望信息化的这个伴随物能够处于我们的认识水平的控制之下。

信息安全工程学便是这样一种控制工具，它强调了信息安全的系统性。用系统工程的观点、方法来对待和处理信息安全问题，是最近一段时间以来信息安全界热切关注的一个焦点。站在信息安全工程的高度上来全面构建和规范我国的信息安全，不但具有重要的理论意义，更将极大地保障国家信息资源的安全。

为此，我们编写了这本《信息安全工程导论》。

其名曰导论，自然指明了这本书不是包罗万象的信息安全知识的罗列，它面向信息安全工程，重在探讨信息安全工程的内容和内涵。信息安全知识具有前所未有的综合性，即使在信息安全工程这样一个非常具体的领域中，也难以通过一本书而阐明其全部内容，更何况这是一个正在迅速发展的领域。因此我们希望这本书能起到抛砖引玉的作用，使更多的人能够加入到信息安全工程的研究和实践中来，共同为加强我国的信息安全保障而努力奋斗。

本书第 1 章简介了信息安全的基本概念，这虽不是本书的主要内容，但我们认为，发展到今天的信息安全仍然有大量的基本概念需要探讨，这些概念对理解信息安全工程至关重要。第 1 章末引出了信息安全工程方法，并简单回顾了信息安全工程方法的发展史。第 2 章阐述了信息安全工程方法的基础——系统工程过程，并随后在第 3 章介绍了在其之上发展而来的信息系统安全工程（ISSE）。第 4 章分析了 ISSE 与其他几个工程过程之间的关系；其后，我

们谈到了与 ISSE 相对的另外一种信息安全工程方法：系统安全工程—能力成熟度模型（SSE-CMM），它已经成为信息安全工程的国际标准，代表了信息安全工程方法发展的优秀成果，这是本书的一项重点内容。我们在第 5 章分析了包括其体系结构在内的 SSE-CMM 方法学，对其应用方法等背景信息做了介绍，并在第 6、7 两章分别阐述了其体系结构中的过程域维和能力维，它们由重要的信息安全工程过程活动所组成。第 8 章分析了 SSE-CMM 对信息安全问题的覆盖面，重点研究了其保证要求。第 9 章的主题是信息安全工程与我国的计算机信息系统安全等级保护的关系。鉴于等级保护制度已开始在我国实施，等级信息安全工程能力将成为等级保护制度中的一个关注重点，因此该章除介绍了信息安全评估与等级保护的背景知识外，还分析了国内正在制定的信息安全工程标准与 SSE-CMM 的关系。第 10 章通过对 ISO/IEC 15443《IT 安全保证框架》的分析，我们强调了以开放思维研究信息安全工程方法的必要性。

附录中除正文的索引信息外，还特别加入了美国国家标准和技术研究所发布的《IT 安全工程原则》中确立的 33 条信息安全工程原则以及 SE-CMM（系统工程-能力成熟度模型）中的 11 个过程域，以供读者参考。

参加本书编写工作的还有左晓栋和蔡谊，此外，刘毅、郑志蓉、陈泽茂、孙锐、盛可军等同志也为本书的编写做了很多工作。本书全稿由赵战生教授审校。

本书受到了国家重点基础研究发展规划项目（973）G1999035801 和国家科学技术学术著作出版基金委员会的支持。

中国工程院院士 沈昌祥

2003 年 6 月

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章 引 言

1.1 信息安全保障的基本概念

1.1.1 什么是信息安全

信息化的迅速发展正在对国家和社会的各方面产生巨大影响，随着国家信息化的不断推进与当前电子政务的大力建设，信息已经成为最能代表综合国力的战略资源。然而，伴随而来的信息安全问题也随之突显。能否有效地保护信息资源，保护信息化进程健康、有序、可持续发展，直接关乎国家安危，关乎民族兴亡，是国家、民族的头等大事。没有信息安全，就没有真正意义上的政治安全，就没有稳固的经济安全和军事安全，更没有完整意义上的国家安全。

那么，如何去理解信息安全呢？这是一个与时俱进的概念，随着时代的发展，信息安全涉及的内容在不断延展，对信息安全的评价标准也在不断变化，这便导致了不同的人、在不同的场合下形成了对信息安全的多方面理解。

因此，孤立地讨论信息安全没有实际意义。信息安全是信息技术发展过程之中提出的课题，在信息化的大背景下被推上了历史舞台。众所周知，信息革命是继人类社会农业革命、工业革命之后的又一次伟大的生产力革命。这种生产力革命的意义，便在于信息已经成为信息社会中须臾不可或缺的基本生活要素，已经成为一种资源。现代战争中，“信息战”的内涵便是围绕着信息这种战略资源的攫取而展开的高技术战争。信息化也是为了最大程度地有效利用信息资源，从而推动社会全面进步。因此，信息安全不是最终目的，它只是服务于信息化的一种手段，其针对的是信息这种战略资源的安全，其主旨在于为信息化保驾护航。

所以，信息安全的概念与信息的本质属性有着必然的联系，它是信息的本质属性所体现的安全意义。经过不断的探索和实践总结，人们首先总结出了信息的三大安全属性：保密性、完整性和可用性。

保密性（Confidentiality）

这是一个古已有之的需要，近代历史上成为战争的情报军事手段和政府的专用技术。在传统信息环境中，普通人通过邮政系统发信件时，为了个人隐私要装上信封。可是到了信息化时代，信息在网上传播时，如果没有这个“信封”，那么所有的信息都是“明信片”，不再有秘密可言。这便是信息安全中的保密性需求。概括地说，保密性是指信息不被泄露给非授权的用户、实体或进程，或被其利用的特性。

常用的保密技术包括：

- 防侦收　使对手侦收不到有用的信息；
- 防辐射　防止有用信息以各种途径辐射出去；
- 信息加密　在密钥的控制下，用加密算法对信息进行加密处理，即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息；
- 物理保密　利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露；
- 信息隐形　将信息嵌入其他客体中，隐藏信息的存在等。

需要指出，保密性不但包括信息内容的保密，还包括信息状态的保密。例如，在军事战争中，即使无法破解对方的加密信息，但仍可从敌方通信流量的骤增情况上推断出某些重要的结论（例如可以推知敌方将有重大军事行动）。确保通信流保密的技术也有很多，例如可以在保证带宽的前提下通过加入大量冗余通信流，从而保持通信流状态的恒定，避免泄密。

信息的保密性往往在信息系统的通信过程中得到相当程度的重视，然而，信息系统在存储与处理中的信息保密问题相当突出，这一点却常为很多人所忽视，应予强调。

完整性（Integrality）

完整性是指信息未经授权不能进行更改的特性。即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响信息完整性的主要因素有：设备故障、误码（例如传输、处理和存储过程中产生的误码，定时稳定度及精度的降低造成的误码，各种干扰源造成的误码）、人为攻击、计算机病毒等。

保护信息完整性的主要方法有：

- 协议　通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。
- 纠错编码方法　由此完成检错和纠错功能。最简单和常用的纠错编码方法是奇偶校验法。
- 密码校验和方法　它是抗篡改和传输失败的重要手段。
- 数字签名　保障信息的真实性，说明其未受到篡改。
- 公证　请求管理或中介机构证明信息的真实性。

可用性（Availability）

可用性是信息可被授权实体访问并按需求使用的特性。例如，在授权用户或实体需要信息服务时，信息服务应该可以使用，或者是信息系统部分受损或需要降级使用时，仍能为授权用户提供有效服务。可用性一般用系统正常使用时间和整个工作时间之比来度量。

信息的可用性与硬件可用性、软件可用性、人员可用性、环境可用性等方面有关。硬件

可用性最为直观和常见。软件可用性是指在规定的时间内，程序成功运行的概率。人员可用性是指人员成功地完成工作或任务的概率。人员可用性在整个系统可用性中扮演着重要角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可用性的重要保障。环境可用性是指在规定的环境内，保证信息处理设备成功运行的概率。这里的环境主要是指自然环境和电磁环境。

以上 3 类信息安全属性在世界范围内得到了共识，各国专家对此均无异议。但是，对于信息安全的其他属性，信息安全界内则没有统一的意见。在我国强调较多的还有信息的可控性与不可否认性。

可控性（Controllability）

由于社会中存在不法分子，世界各国之间还时有由于意识形态和利益冲突造成的敌对行为。政府对社会的监控管理行为（如搭线监听犯罪分子的通信），在社会广泛使用信息安全设施和装置时可能受到严重影响，以至不能实施，这就出现了信息安全中的可控性需求。

概括说来，信息安全的可控性是指能够控制使用信息资源的人或实体的使用方式。对于信息系统中的敏感信息资源，如果任何人都能访问、篡改、窃取以及恶意散播的话，那么安全系统显然失去了效用。对访问信息资源的人或实体的使用方式进行有效的控制，是信息安全的必然要求。

从国家的层面看，信息安全中的可控性不但涉及到了信息的可控，还与安全产品、安全市场、安全厂商、安全研发人员的可控性密切相关。

不可否认性（Non-repudiation）

不可否认性也称抗抵赖性。它是传统社会的不可否认需求在信息社会中的延伸。

人类社会中的各种商务行为均建立在信任的基础之上。没有信任，也就不存在人与人之间的交互，更不可能有社会的存在。传统的公章、印戳、签名等手段便是实现不可否认性的主要机制。

信息的不可否认性与此相同，也是防止实体否认其已经发生的行为，只不过这个时候的实体位于信息空间中。与传统社会相同，不可否认性分为原发不可否认（也称原发抗抵赖）和接收不可否认（也称接收抗抵赖）。前者用于防止发送者否认自己已发送的数据和数据内容；后者防止接收者否认已接收过的数据和数据内容。

实现不可否认性的手段与技术有很多，最常用的是数字证书和数字签名技术。

在国外（尤以美国为例），除强调信息的保密性、完整性、可用性之外，还常常谈到“可追究性（Accountability）”，也有将其译作“可核查性”，指确保某个实体的行动能惟一地追溯到该实体。进一步，又可将可追究性分为“鉴别”与“不可否认性”，前者要求“验证用户和发送者的身份”，后者要求“用户和发送者不能否认自己的行为”。显然，可追究性与国内提倡的不可否认性是一致的，它也部分体现了信息的可控性需求。

经如上分析，可以将信息安全定义为“保护信息和信息系统不被未经授权的访问、使用、泄露、中断、修改和破坏，为信息和信息系统提供保密性、完整性、可用性、可控性和不可否认性”。

欧共体方面则将信息安全定义为“在既定的密级条件下，网络与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或传输的数据以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和秘密性”。

目前，世界上尚未对信息安全的定义达成一致，甚至“信息安全”本身的称谓也在改变。例如，美国军方自20世纪90年代末便将“信息安全”的概念发展成“信息保障”，突出了信息安全保障系统的多种安全能力及其对机构业务职能的支撑作用；美国政府在近年来也多在更为广阔“cyber安全”的概念下讨论信息安全问题，表明其看待信息安全问题的视角已经不再局限于单个维度，而是将信息安全问题抽象为一个由信息系统、信息内容、信息系统的所有者和运营者、信息安全规则等多个因素构成的一个多维的问题空间。这些变化均反映出了人们对信息安全的意义、内容、实现方法等一直在不断地思索和实践。

但就本质而言，不论使用何种称谓和定义，所针对的均是“信息”这种资源的“安全”，对信息安全的理解应从信息化背景出发，最终落实在信息的安全属性上。

1.1.2 信息安全的发展过程

信息的上述若干安全属性没有出现在同一历史时期，而是与信息技术的发展相伴，受到了不同历史时期应用需求的驱动。本节将集中回顾信息安全所走过的道路。

普遍认为，现代信息安全的发展可以划分为3个阶段。

1.1.2.1 通信保密阶段（COMSEC）

通信保密阶段的开始时间约为20世纪40年代，其时代标志是1949年Shannon发表的《保密系统的信息理论》，该理论将密码学的研究纳入了科学的轨道。在这个阶段所面临的主要安全威胁是搭线窃听和密码学分析，其主要的防护措施是数据加密。

在该阶段人们关心的只是通信安全，而且主要关心对象是军方和政府。需要解决的问题是在远程通信中拒绝非授权用户的信息访问以及确保通信的真实性，包括：加密、传输保密、发射保密以及通信设备的物理安全，通信保密阶段的技术重点是通过密码技术解决通信保密问题，保证数据的保密性和完整性。当时涉及的安全性有：保密性，保证信息不泄露给未经授权的人或设备；可靠性，确保信道、消息源、发信人的真实性以及核对信息接收者的合法性。

在当时，虽然计算机系统的脆弱性已日益为美国政府和私营部门的一些机构所认识，但由于当时计算机的速度和性能比较落后，使用范围有限，加之美国政府将其作为敏感问题而加以控制，因此，有关计算机安全的研究一直局限在比较小的范围内。

1.1.2.2 计算机安全（COMPUSEC）和信息安全阶段（INFOSEC）

进入20世纪70年代，通信保密阶段转变到计算机安全阶段。这一时代的标志是1977年美国国家标准局（NBS）公布的《国家数据加密标准》（DES）和1985年美国国防部（DoD）公布的《可信计算机系统评估准则》（TCSEC）。这些标准的提出意味着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。

进入20世纪80年代后，计算机的性能得到了成百上千倍的提高，应用的范围也在不断扩大，计算机已遍及世界各个角落。而且人们正努力利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。但是，随之而来并日益严峻的问题是计算机信息的安全问题。人们在这方面所做的研究与计算机性能和应用的飞速发展不相适应，因此，它已成为未来信息技术中的主要问题之一。

由于计算机信息有共享和易于扩散等特性，它在处理、存储、传输和使用上有着严重的脆弱性，很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、冒充和破坏。

于是该阶段最初的重点是确保计算机系统中的硬件、软件及在处理、存储、传输信息中的保密性。主要安全威胁是信息的非授权访问，主要保护措施是安全操作系统的可信计算基技术（TCB），其局限性在于仍旧没有超出保密性的范畴。

TCSEC将计算机安全与操作系统可信计算基紧密联系在了一起，通过访问控制防止对信息的非授权访问，从而保护信息的保密性，其思想至今仍对安全操作系统的研究具有指导意义。但是，随着计算机病毒、计算机软件Bug等问题的不断显现，保密性已经不足以满足人们对计算机安全的需求，完整性和可用性等新需求于是开始出现。

此后，国际标准化组织（ISO）将“计算机安全”定义为：“为数据处理系统建立的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。”也有人将“计算机安全”定义为：“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。”就计算机安全而言，这些概念已经比较全面，但它们的关注对象仍没有离开计算机。

20世纪90年代以来，通信和计算机技术相互依存，数字化技术促进了计算机网络发展成为全天候、通全球、个人化、智能化的信息高速公路，Internet成了寻常百姓可及的家用技术平台，安全的需求不断地向社会的各个领域扩展，人们的关注对象已经逐步从计算机转向更具本质性的信息本身，信息安全的概念随之产生。人们需要保护信息在存储、处理或传输过程中不被非法访问或更改，确保对合法用户的服务并限制非授权用户的服务，包括必要的检测、记录和抵御攻击的措施。于是除保密性、完整性和可用性之外，人们对安全性有了新的需求：可控性和不可否认性。

计算机安全过渡到信息安全后，世界各地的安全文献已经很少谈及计算机安全，多代之以“IT安全”。

这一时期，在密码学方面，公钥技术得到了长足的发展，著名的RSA公开密钥密码算法获得了日益广泛的应用，用于完整性校验的Hash函数的研究应用也越来越多。为了奠定21世纪的分组密码算法基础，美国国家技术和标准研究所（NIST）推行了高级加密标准（AES）的项目，1998年7月选出了15种分组密码算法作为候选算法。继而经过广泛评价，从中进一步选出了5个较好的算法。经过更加广泛和严谨的评审后，5个算法中的Rijndael胜出，最终成为了AES算法。另外，人们已经把更强更快的公钥密码算法的研究和应用投向了椭圆曲线公开密钥密码算法上。

虽然该阶段包括了计算机安全和信息安全两个不同的阶段，但它们的时间区分不明显，可将其统称为INFOSEC阶段。

1.1.2.3 信息保障阶段（IA）

时至今日，对于信息系统的攻击日趋频繁，安全的概念逐渐发生了两个方面的变化：

- 安全不再局限于信息的保护，人们需要的是对整个信息和信息系统的保护和防御，包括了保护、检测、反应和恢复能力（PDRR）；
- 安全与应用的结合更加紧密，其相对性、动态性等特性日趋引起注意，追求适度风险的信息安全成为共识，安全不再单纯以功能或机制的强度作为评判指标，而是结合了应用环境和应用需求，强调安全是一种信心的度量，使信息系统的使用者确信其预期的安全目标已获满足。

于是美国军方提出了信息保障（IA）的概念：“保护和防御信息及信息系统，确保其可用性、完整性、保密性、鉴别、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。”（美国国防部令S-3600.1）

信息保障除强调了信息安全的保护能力外，还提出要重视提高系统的入侵检测能力、系统的事件反应能力以及系统在遭到入侵引起破坏后的快速恢复能力。它关注的是信息系统整个生命周期的防御和恢复。这样一个由保护、检测、反应、恢复等内容构成的框架如图1-1所示。

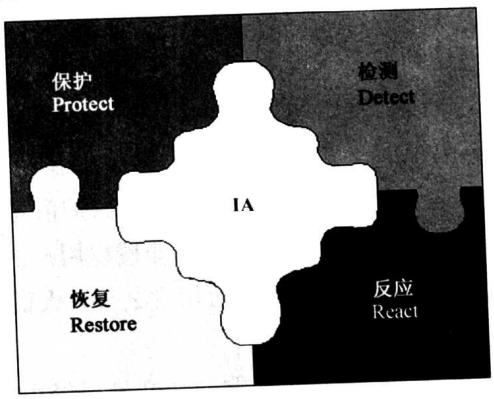


图1-1 信息保障的四大功能

此为试读，需要完整PDF请访问：www.ertongbook.com