Fundamental Information Security Course

信息安全保密基础教程

主　编　施　峰　副主编　胡昌振　刘炳华

国防科技工业保密资格审查认证中心

Fundamental Information Security Course

Fundamental Information Security Course

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

图书在版编目（CIP）数据

信息安全保密基础教程/施峰主编. —北京：北京理工大学出版社，2008.5

ISBN 978-7-5640-1468-1

Ⅰ. 信…　Ⅱ. 施…　Ⅲ. 信息系统-安全技术-教材　Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2008）第 036018 号

出版发行／北京理工大学出版社
社　　址／北京市海淀区中关村南大街 5 号
邮　　编／100081
电　　话／(010) 68914775(办公室)　68944990(批销中心)　68911084(读者服务部)
网　　址／http：//www. bitpress. com. cn
经　　销／全国各地新华书店
印　　刷／北京圣瑞伦印刷厂
开　　本／787 毫米×1092 毫米　1/16
印　　张／34.5
字　　数／835 千字
版　　次／2008 年 5 月第 1 版　2008 年 5 月第 1 次印刷
印　　数／1～3000 册　　责任校对／陈玉梅
定　　价／112.00 元　　责任印制／母长新

前　言

随着我国社会主义市场经济的逐步完善和国防科技工业寓军于民体制改革的不断深入，特别是信息化建设的推进和应用，国防科技工业安全保密工作凸显重要。特别是在信息技术飞速发展的今天，“敌我双方零距离，敌我双方共桌面”，境内外敌对势力加大了对我国国防科技工业涉密信息系统的攻击和情报窃密，信息安全保密形势十分严峻，加强安全保密能力建设刻不容缓。

安全是基础，保密是核心。信息安全与保密是国防科技工业的核心竞争力之一，如果没有坚实的信息安全基础，则无异于把国防科技工业国家秘密信息拱手与人共享。国家利益高于一切，保密责任重于泰山。正是为了确保国家秘密信息安全，国防科技工业保密资格审查认证中心在国防科工委、国家保密局、北京理工大学、南京航空航天大学等单位的指导和帮助下，结合军工企事业单位安全保密工作的实际，组织编写了《信息安全保密基础教程》，旨在对国防科技工业信息安全保密进行积极的理论和实践探索，特别是针对信息系统管理员、安全保密管理员、安全审计员的“三员”进行培训。因为“三员”是涉密信息系统的管理者，掌握着大量的国家秘密，他们的安全保密意识与管理水平及业务素质直接关系到涉密信息系统的安全，如果其中“一员”发生问题都将给国家安全和利益造成重大损失。因此，开展对“三员”的安全保密培训，既是切实提高涉密信息系统安全保密管理水平的需要，也是加快国防科技工业安全保密能力建设的关键。

本教程由国防科技工业保密资格审查认证中心组织编写。中国国防科技信息中心刘炳华研究员、航天科工706所王晓程高级工程师、航天科技710所经小川博士、国家信息中心范红博士、中船重工716所陈双龙研究员、中国船舶综合技术经济研究院佟占杰高级工程师、南京航空航天大学庄毅教授、刘佳博士、许峰博士、王箭博士、袁家斌博士、黄玉划博士和夏正友副教授、北京理工大学闫怀志博士和孙建伟博士等专家参加了编写。

在教程编写过程中，国防科技工业保密资格审查认证中心的葛杨高级工程师、黄次辉、黄欣、周铁工程师，以及北京理工大学的方平副教授等提供了具体的指导和帮助，在此表示衷心的感谢。

由于时间仓促，水平有限，本教程难免存在疏漏和不足之处，欢迎批评指正。

国防科技工业保密资格审查认证中心

施峰

2007年7月16日

目　录

第1章　信息安全与保密基本知识

1.1 引　　言

在信息化建设过程中，最重要的问题是解决好信息安全和保密。目前，我国的信息安全保障工作正在逐步加强，制定并实施了国家信息安全战略，初步建立了信息安全管理体制，基础信息网络和重要信息系统的安全防护水平明显提高，互联网信息安全管理得到进一步加强。

信息安全与保密工作需要坚持不懈的长期努力。目前，从全球范围看，计算机病毒、网络攻击、垃圾邮件、系统漏洞、网络窃密、虚假有害信息和网络违法犯罪等问题日渐突出。根据我国公安部公共信息网络安全监察局在 2005 年举办的计算机病毒疫情网上调查的结果显示，自 2001 年以来，我国的计算机病毒感染率一直处于较高水平。2001 年感染过计算机病毒的用户数量占被调查总数的 73%，2002 年为 83.98%，2003 年增长到 85.57%，2004 年的病毒感染率高达 87.93%，2005 年稍有回落，为 80%。根据我国网络域名管理中心关于互联网入侵调查情况的统计数据可以看出，我国网络被入侵的情况是不容乐观的，2001 为 44.66%，2002 年为 63.3%，2003 年为 59.43%，2004 年为 49%。针对这一情况，2006 年 5 月中共中央办公厅、国务院办公厅联合印发了《2006—2020 年国家信息化发展战略》文件，明确指出：将“建设国家信息安全保障体系”作为国家信息化发展战略的重点之一。要全面加强国家信息安全保障体系建设，大力提高国家信息安全的保障能力，坚持推进信息化建设与保障国家信息安全并重的原则，不断提高基础信息网络和重要信息系统的安全保护水平。以达到“信息安全的长效机制基本形成，国家信息安全保障体系较为完善，信息安全保障能力显著增强”的战略目标。

1.2 信息安全与保密的基本概念

1.2.1 信息安全与保密的定义和发展

一、信息安全与保密的定义

（一）信息安全

信息安全是指对信息系统的硬件、软件以及数据信息实施安全防护，保证在意外事故或恶意攻击情况下系统不会遭到破坏、敏感数据信息不会被篡改和泄漏，保证信息的机密性、完整性、可用性和可控性，并保证系统能够正常运行，信息服务功能不中断。

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漏与扩散。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，运行过程中不出现故障，并且在遇到意外情况时能够尽量减少损失，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。

信息安全面临的威胁非常广泛，如信息泄漏、非法使用、窃听、假冒、重放、抵赖等，要确保信息的安全性主要应解决好以下问题：安全漏洞与安全对策问题、网络攻击与攻击检测、防范问题、病毒防治问题、数据备份与恢复问题、灾难恢复问题、实体保护问题等。

（二）保密

保密是人类社会进入文明时代产生私有制观念条件下形成的意识以及由这种意识支配而产生的社会行为。从国家安全利益的角度，保密泛指保守党和国家的秘密。《中华人民共和国保守国家秘密法》（以下简称《保密法》）第二条将国家秘密明确定义为“关系国家的安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项”。第八条同时规定：“国家秘密包括符合本法第二条规定的下列秘密事项：（一）国家事务的重大决策中的秘密事项；（二）国防建设和武装力量活动中的秘密事项；（三）外交和外事活动中的秘密事项以及对外承担保密义务的事项；（四）国民经济和社会发展中的秘密事项；（五）科学技术中的秘密实项；（六）维护国家安全活动和追查刑事犯罪中的秘密事项；（七）其他经国家保密工作部门确定应当保守的国家秘密事项。政党的秘密事项中符合本法第二条之规定，属于国家秘密。”保守国家秘密指严格按照党和国家的保密法律、法规、制度的规定和要求，将涉密信息及涉密信息载体（如公文、档案、物品等）控制在一定范围内使用，限制不应知悉的人员知悉，同时也包含了组织和个人为国家保守秘密的职责和所采取的保守秘密的措施和活动。一般来说，凡是列入保密范围的涉密信息，都有比较明确的保密期限，在保密期限内，其知悉范围是通过强制性手段和措施来控制的。

对国家秘密信息进行采集、加工、存储、传输、检索等处理的计算机信息系统统称为“涉密计算机信息系统”，简称“涉密系统”。对非国家秘密信息进行处理的计算机信息系统，称为“非涉密系统”。

计算机信息系统的安全保密是指为了防止泄密、窃密和破坏，对计算机信息系统及其所存储的信息和数据、相关的环境与场所、安全保密产品进行安全防护，确保以电磁信号为主要形式的信息在产生、存储、传递和处理等过程中的保密性、完整性、可用性和抗抵赖性。一个安全保密的计算机信息系统，应能达到“五不”：“进不来、拿不走、看不懂、走不脱、赖不掉”。即非法用户进入不了系统；非授权用户拿不到信息；对重要的信息进行加密，即使非授权者看见了也看不懂；若别有用心的人一旦进入了系统或在涉密系统内进行违规操作，必将留下痕迹，无法逃脱；即便有信息被拿走或篡改了，系统的安全保密机制将自动产生相关记录和证据。

为了做好信息安全保密工作，我国制定了相关的政策和原则。我国信息安全保密的总政策是：① 统一领导，严格管理；② 定点研制，专控经营；③ 满足使用，确保安全；④ 自主开发，突出特色；⑤ 大力发展，形成产业。

二、信息安全认识的发展过程

人们对信息安全的认识是随着信息系统技术的发展和应用而逐步深化的，主要经历了信息保密、信息保护和信息保障三个发展阶段。

（一）信息保密

20 世纪 80 年代以前，人们对信息安全的认识仅停留在信息保密的层次上。信息保密是人们最早认识到的安全需要。信息保密的手段除了采取保密管理措施外，在技术方面主要采用密码技术，对传输的信息进行加密处理，并对信息系统的进入和数据的读取采用访问控制和授权管理方法。即一方面要对系统中存储的数据信息进行保密，另一方面则要求对通信双方传输交换的信息进行保密，其中特别要重视通信过程中端到端的安全保密。这一时期的重要技术发展标志有：1977 年美国国家标准局（NBS）公布的国家数据加密标准（DES）和 1983 美国国防部公布的可信计算机系统评价准则（Trusted Computer System Evaluation Criteria，TCSEC，俗称橘皮书）。DES 算法是密码学历史上第一个公布了内部实现细节的密码算法，它的安全只依赖于算法的密钥，使得算法可以被更广泛地应用于各种场合；而 TCSEC 则提出了基于科学的访问控制模型的可信信息系统的等级化要求。它们的出现意味着解决计算机信息安全和保密问题的研究和应用迈上了历史的新台阶。

（二）信息保护

20 世纪 80 年代至 90 年代之间，计算机网络逐步产生并发展起来，计算机系统成为信息安全的主要保护对象。计算机系统通常定义为由计算机及其相关的配套设备、设施构成的，按照一定的应用目标和规格对信息进行采集、加工、存储、传输、检索等处理的系统。它主要由硬件系统和软件系统两个部分组成，硬件系统包括计算机、网络设备及其他配套设备；软件系统则主要包括系统软件、工具软件和应用软件。在这一时期，人们认识到除了信息保密的需要外，信息是否在存储、处理和传输的过程中被未经授权者进行插入、删除、修改，是否在需要使用的时间、地点可以使用，也是信息安全的重要需求。因此，根据这些新的需求提出了保密性以外的另外两个安全属性——“完整性”和“可用性”，并把信息安全共识为信息的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。

（三）信息保障

20 世纪 90 年代以后，随着 Internet 的全球化发展和应用，在数字化、网络化、个性化的应用环境中如何确认人们的身份和责任成为应用中必须考虑的新问题。为了解决这些新问题提出了新的安全属性——可认证性（Authenticity）、不可否认性（Non-repudiation）和可追究性（Accountability）等。人们认识到单纯的被动保护已不能适应全球化网络数字环境的安全需要，因此信息保障（IA-Information Assurance）的概念随之被提出，并在保护（Protect）、检测（Detect）、响应（React）和恢复（Restore）四个环节的基础上提出了“纵深防御”的思想。

1.2.2　信息安全的基本属性

一、信息系统的基本属性 CIA

信息系统主要有保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）这三个基本属性。

（一）保密性

保密性是指保证信息不会泄漏给非授权用户、实体或者进程。保密性具有以下三个方面的特性：

（1）保密是相对于信息的非授权范围而言的。不论是国家、单位、团体、个人都存在着

其专有信息和秘密，这些信息只能在一定范围内公开，而对非授权范围应严格地进行保密控制。

（2）保密要求有不同的等级。国家保密法界定了绝密、机密、保密三个基本等级。在信息系统中，为了完成工作使命的要求，通常对等级进行更细粒度的划分，并有针对性地采取不同力度的保护。

（3）保密不仅是针对人，信息系统带来了信息生存的数字化环境，对存储、传输、打印和复印等设备的使用也必须根据安全策略的要求，实施严格的保密控制。

目前，常用的保密技术有：

（1）物理保密。利用各种物理方法，如限制、隔离、隐蔽、控制等措施，保护信息不被泄漏；

（2）防窃听。使对手侦听不到有用的信息；

（3）防辐射。防止有用信息以各种途径辐射出去；

（4）信息加密。采用加密算法对信息进行加密处理。使对手即使得到了加密后的信息也会因为没有密钥而无法读懂有效的信息。

（二）完整性

完整性是指信息在存储或传输过程中保持不被未授权的、非预期的或无意的操作修改和破坏。完整性要求保持信息的原始面貌，即信息的正确生成、正确存储和正确传输。完整性不仅包括数据完整性，还包括系统完整性。系统完整性反应了操作系统的逻辑正确性和可靠性，实现保护机制的硬件和软件的逻辑完备性以及数据结构和数据存储的一致性。

完整性的破坏来自三个方面的影响：未授权操作、非预期操作和无意操作。在技术应用过程中除了人为的恶意破坏外，还存在由于能力和素质达不到要求而造成的无意误操作和由于系统程序漏洞而造成的非预期误动作问题，它们同样会影响信息的完整性，需要采取完整性保护措施来加以防范。目前，保障完整性的方法主要有以下几种：

（1）良好的协议。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；

（2）采用密码校验和。密码校验和是抗篡改和传输失败的重要手段；

（3）数字签名。采用数字签名技术既可保障信息的完整性，同时又可保证信息的不可否认性；

（4）可信第三方。请求网络中通信双方所共同信任的第三方进行信息完整性的证明。

（三）可用性

可用性指信息可以被授权者访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性；或者是当网络部分受损或需要降级使用时，仍能为授权用户提供部分有效服务的特性。可用性一般采用系统正常使用时间和整个工作时间之比来度量。对可用性的攻击主要通过阻断信息合理使用的方法完成，例如破坏系统的正常运行就属于这种类型的攻击。目前，保证可用性的方法主要有：

（1）访问控制。对用户的权限进行控制，使其只能访问相应权限的资源，防止或限制经隐蔽通道进行的非法访问；

（2）业务流控制。利用均分负荷方法，防止业务流量过度集中而引起的网络阻塞。如大型 ISP 提供的电子邮件服务，一般有多个邮件服务器进行负载均衡；