信息安全理论与技术

薛丽敏 陆幼骊
罗 隽 丁 霞 林晨希 编著

国防工业出版社
National Defense Industry Press

信息安全理论与技术

薛丽敏　陆幼骊
罗　隽　丁　霞　林晨希　编著

国防工业出版社
·北京·

内容简介

本书从信息系统与网络的安全威胁和安全需求分析着手，阐述了信息安全体系结构、信息安全策略和信息安全模型，以及信息安全保障的核心——密码学基础知识。在深入分析和研究计算机病毒等恶意代码的基础上，论述了防火墙、入侵检测、访问控制、安全协议等网络安全防护技术，特别是入侵防御、统一威胁管理、可信计算平台和网格安全等动态的、先进的信息网络安全保障新技术，以及无线网络的安全性问题；最后从信息安全工程、信息安全风险评估、网络安全事件响应、容灾技术和安全评价标准等方面对信息安全工程保障和信息安全管理保障进行了系统的探讨。

本书主要面向计算机、通信等专业、关注信息安全方向的硕士研究生，是一本介绍信息网络环境中信息安全的专业理论教材，也可以作为信息安全专业的本科生、研究信息战和信息安全理论的科研人员的参考用书。

图书在版编目(CIP)数据

信息安全理论与技术/薛丽敏等编著. —北京：国防工业出版社，2014.10

ISBN 978-7-118-09662-0

Ⅰ. ①信… Ⅱ. ①薛… Ⅲ. ①信息安全—安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2014)第 230307 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 19¾ **字数** 477 千字

2014 年 10 月第 1 版第 1 次印刷 **印数** 1—3000 册 **定价** 58.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

前　言

信息化战争是以现代化的指挥、控制、通信、计算机、情报、监视、侦察，即 C^4ISR 系统为主的网络化信息系统，把陆、海、空、天战场联成一个巨大的全维作战网络，将实现作战信息获取、传输、处理一体化，作战空间多维一体化，作战力量合成一体化，作战行动协调一体化。因此，信息化战争首要是通过破坏对手信息系统和网络来破坏作战体系一体性，通过保护己方信息系统和网络的安全来保证作战体系和一体性，只有这样才能打赢信息化战争。为达到上述目标，就必须认真研究信息网络安全保障技术。本书正是面向这个迫切需求开展研究和编著的。

信息安全发展至今，从强调对抗针对信息及信息系统的各种威胁所必要的措施，到强调信息系统的保护、检测和恢复能力（信息安全保障 Information Assurance，IA），其本质是从被动的、静态的措施，到主动的、动态的能力。因此，信息安全保障是信息安全理论的重要发展，其目标是使系统从组建到运行的整个生命周期中都满足安全需求。

本书的编著是将信息网络安全作为一个系统工程，综合集成于一体，进行深入研究、探讨和阐述的。同时，本着“基础、前沿、应用”兼顾的思想，以信息安全基本理论为基础，分别从技术、工程和管理三个方面展开对信息安全保障思想、技术及方法的论述，力求由浅入深，内容简练，体系较为完整。

本书共 13 章，第 1、2、6、7、9、13 章主要由薛丽敏编写；第 3、4 章主要由陆幼骊编写；第 5 章主要由林晨希编写；第 8、12 章主要由罗隽编写；第 10、11 章主要由丁霞编写，宋庆帅完成插图。另外，王来和赵俊阁、赵守连和刘明给本书的编写、校对工作提供了宝贵的建议和大量的帮助，在此表示感谢！

作者在编写本书时，曾直接或间接地引用了许多专家、学者的文献和著作，在此向他们深表谢意。

由于篇幅受限，再加上作者学识有限，还有时间仓促，疏漏和不妥之处在所难免，恳请读者不吝指教。

编著者

2014 年 6 月

目　录

第 1 章　信息安全基础理论

信息技术的发展带动了全球信息化的发展，信息基础设施已成为社会基础设施中必不可少的关键基础设施。而广泛普及的 Internet，在给人们带来巨大便利的同时，信息的安全与保密问题日益突出。具体表现有：黑客攻击搅得全球不安，已由零散的个人行为发展成为有组织的团队行为；计算机病毒网上肆虐；白领犯罪造成巨大商业损失；数字化能力的差距造成世界上不平等竞争，信息战阴影威胁数字化和平。正所谓“Internet 最大的好处是将你和所有人都连在一起；Internet 最大的坏处也是将你和所有人都连在一起”。

因此，许多专家认为“ 威胁是客观存在的事实”。信息战是 Internet 发展的一个必然结果，是人们生活在信息经济中付出的代价之一。信息战的要点之一就是保证己方的信息安全，打击敌方的信息安全。

那么什么是信息安全呢？

信息安全的含义大致可以分成两大类：一类是指具体的信息技术系统的安全；另一类是指某一特定信息体系（如一个国家的银行信息系统、军事指挥系统等）的安全。

广义上，信息安全是指“一个国家的社会信息化状态和信息技术体系不受外来的威胁与侵害。

狭义上，信息安全可以定义为：保护信息及信息系统在信息存储、处理、传输过程中不被非法访问或修改，而且对合法用户不发生拒绝服务。信息安全包括检测（探测）、记录、对抗此类威胁所必要的措施。

从产生到现在，信息安全的发展经历了这样几个过程：

（1）通信保密（COMSEC）：20 世纪 60 年代以前，主要是在通信的收发双方加入了加密这一环节。

（2）计算机安全（COMPUSEC）：20 世纪 70 年代至 80 年代，主要研究信息的机密性、完整性、可用性，还有安全 OS 技术。

（3）网络信息安全（INFOSEC）：20 世纪 90 年代后，主要研究网络上的信息、信息对抗、虚拟专用网 VPN、公钥基础设施 PKI 和风险评估等。

（4）构造信息安全基础设施等保障体系阶段（IA）：21 世纪，主要为数据备份与灾难恢复技术、国际联动的安全应急响应等。

可以看出，信息安全发展至今，从强调对抗针对信息及信息系统的各种威胁所必要的措施，到强调信息系统的保护、检测和恢复能力，即信息安全保障（Information Assurance，IA），其本质是从被动的、静态的措施，到主动的、动态的能力。因此，信息安全保障是信息安全理论的重要发展，其目标是使系统从组建到运行的整个生命周期中都满足安全需求。

1.1 信息安全需求

在高度信息化的今天，信息战是现代战争的发展趋势和主体形式，实时、非对称、非接触、无间断等已成为现代战争的重要特点。在信息战诸要素中，信息安全是一个重要环节，它直接关系到国家和军队利益，关系到信息作战的成败。随着信息安全保障重要性的日益提高，它在现代战争中已上升为五大作战能力之一。而以计算机为核心的信息网络已经成为现代社会的神经中枢。因此，信息安全与信息安全保障的重点是网络信息安全保障。

1.1.1 网络信息系统的安全威胁

计算机网络所面临的威胁包括对网络中信息的威胁和对网络中设备的威胁。影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；还可能是外来黑客或内部人员（包括信息系统的管理者、使用者和决策者）对网络系统资源的非法使用等，这些可具体分为：内部人员（包括信息系统的开发者、维护者等）、特殊身份人员（具有特殊身份的人，比如审计人员、稽查人员、记者等）、外部黑客及组织、竞争对手、网络恐怖组织、军事组织或国家组织等。

网络资源的军事争夺、军事侦察与军事破坏对战争的胜负有着直接的影响，网络安全本身就是在与网络安全威胁相对抗的过程中形成和发展的，研究信息安全防护必须首先了解对网络安全的威胁。

1. 网络信息安全问题根源

网络信息安全问题源于以下几个方面：

（1）黑客的攻击。目前，世界上有 20 多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用以及系统的一些漏洞，因而系统、站点遭受攻击的可能性就变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性深，“杀伤力”强，这是对网络安全的主要威胁。

（2）管理的欠缺。企业、机构及用户的网站或系统都疏于安全方面的管理。据 IT 界企业团体 ITAA 的调查显示，美国 90% 的 IT 企业对黑客攻击准备不足。目前，美国有 75% ~85% 的网站都抵挡不住黑客的攻击，约有 75% 的企业网上信息失窃，损失惨重。

（3）网络的缺陷。Internet 的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的 TCP/IP 协议族，缺乏相应的安全机制，设计考虑的是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题。

（4）软件的漏洞或“后门”。随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免地存在，常用的操作系统，无论是 Windows 还是 Unix 几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、一些桌面软件都被发现过存在安全隐患。可以说任何一个软件系统都可能会因为程序员的一个疏忽，或设计中的一个缺陷等原因而产生漏洞，这也是网络安全的主要威胁之一。

（5）网络内部的威胁。用户的误操作，资源滥用和恶意行为使得再完善的防火墙也无法

抵御来自网络内部的攻击，也无法对网络内部的滥用做出反应。

2. 网络信息系统面临的安全威胁

（1）非授权访问。非授权访问主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。非授权访问的威胁涉及到受影响的用户数量和可能被泄露的信息。入侵是一件很难办的事，它会动摇人心。而入侵者往往将目标对准政府部门或学术组织。

（2）信息泄漏或丢失是指敏感数据在有意或无意中被泄漏出去或丢失，它通常包括，信息在传输中丢失或泄漏，信息在存储介质中丢失或泄漏，通过建立隐蔽隧道等窃取敏感信息等。具有严格分类的信息系统不应该直接连接 Internet。

（3）破坏数据完整性是指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

（4）拒绝服务攻击。拒绝服务攻击不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

（5）利用网络传播病毒。通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

下面列出了一些典型的威胁以及它们之间的相互关系（图 1－1）。

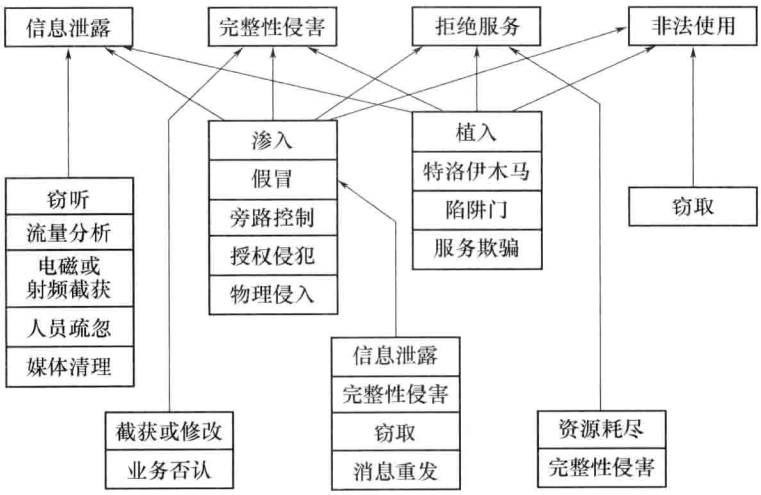

图 1－1　典型威胁及其相互关系

1.1.2　网络信息系统安全的基本需求

网络信息系统安全的内容包括了系统安全和信息安全两个部分。系统安全主要是指网络设备的硬件、操作系统和应用软件的安全；信息安全主要是指各种信息的存储、传输的安全。网络信息系统安全通常依赖于两种技术：一是传统意义上的存取控制和授权，如访问控制表技术、口令验证技术等；二是利用密码技术实现对信息的加密、身份鉴别等。

从网络运行和管理者角度看，希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“后门”、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，进而制止

和防御网络黑客的攻击；而从安全保密部门来看，希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免重要信息泄露，避免对社会产生危害，对国家造成巨大损失。

一般从以下 5 个方面定义网络信息系统安全的基本需求，它也是信息安全的基本属性。

1. 保密性

保密性（Confidentiality）是指信息不泄露给非授权的用户、实体和过程，不被非法利用。攻击中的监听、流量分析就是对系统的保密性进行攻击。军用信息安全尤为注重信息的保密性；比较而言，商用则更注重信息的完整性。

2. 完整性

完整性（Integrity）是指信息在存储或传输过程中，数据未经授权不能进行改变的特性，并且能够判别出数据是否已被改变，例如，保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失等。其目的就是保证信息系统上的数据处于一种完整和未受损的状态，不会因有意或无意的事件而被改变或丢失。攻击中的篡改即是对系统的完整性进行破坏。对于军用信息来说，完整性被破坏可能意味着延误战机、自相残杀或闲置战斗力。

3. 可用性

可用性（Availability）是指可被授权实体访问并按需求使用的特性，即当需要时授权者总能够存取所需的信息，攻击者不能占用所有的资源而妨碍授权者的使用。网络环境下的拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。但要保证系统和网络中能提供正常的服务，除了备份和冗余配置外，目前没有特别有效的方法。

4. 可控性

可控性（Controllability）是指可以控制信息的机密性，控制授权范围内的信息流向及行为方式，对信息的传播及内容具有控制能力。为保证可控性，首先，系统能够控制谁能够访问系统或网络上的数据，以及如何访问（是只读还是可以修改等），通常通过访问控制列表等方法来实现；其次，需要对网络上的用户进行验证，可通过握手协议和鉴别进行身份验证；最后，要将用户的所有活动记录下来便于查询审计。美国政府所提倡的“密钥托管”“密钥恢复”等措施就是实现信息安全可控性的例子。

5. 不可否认性

不可否认性（Non - Repudiation）是指信息的行为人要对自己的信息行为负责，不能抵赖自己曾有过的行为，也不能否认曾经接到对方的信息，因此又称为不可抵赖性。这在交易系统中十分重要。通常将数字签名和公证机制一同使用来保证不可否认性。

1.2 信息安全体系结构

由上可知，以计算机网络为核心的信息系统的安全已成为信息时代人们关注的重要问题之一，而解决信息安全问题的要点是进行顶层设计，自顶向下地设计信息系统的安全子系统，信息安全体系结构正是遵循这一原则，从整体上解决信息系统的安全问题。

1.2.1 安全体系结构理论

1. 安全体系结构的概念

网络安全体系结构与网络体系结构在概念上是紧密相连的。体系结构的含义取决于其实

际应用范围和背景，有时是指各组成单元及其相互关系，以及制约各单元设计和演进的原理和指南，有时也可以指一个系统或部分的组织结构等。“计算机体系结构”不是研究具体的计算机硬件和软件，而是从整体上抽象计算机的逻辑构造和功能，用于指导计算机的设计、生产和软件配置。“计算机网络体系结构”是指由网络实体、层和协议等要素构成的网络功能层次化结构模型以及各要素之间的关系，或者用来统称网络的层次结构、协议栈和相邻层间的接口及服务等。“网络安全体系结构”也不是研究具体的网络安全硬件和软件，而是从整体上抽象网络安全的逻辑构造和功能，用于指导网络安全的整体设计、部署、软件配置和管理。

2. 安全体系结构的理论基础

信息网络安全体系结构的理论基础是整体论、系统论、“木桶”理论。

整体论强调整体功能大于部分功能和，主要处理整体与部分的关系。整体功能的发挥依赖于各部分的密切配合与通力协作，即整体中各部分要有自己强大的功能，各部分之间要有无缝的连接。在整个安全防护中，功能相对较弱的部分以及各部分之间的协作程度对系统的整体安全防护起着至关重要作用，要有针对性地加以改进。

系统论强调系统中各元素功能的密切协作。系统元素的协作性是系统功能的基础，任何单一元素或一部分元素的组合都不具有系统功能。在信息安全系统中，所有各部分的协作联动是保障安全的最佳结构。

1.2.2 信息安全体系结构

网络安全体系结构与网络的体系结构是密切相关的。安全体系结构要把信息安全因素加入到系统的体系结构中，描述系统在满足安全性需求方面各基本要素之间的关系，即描述系统如何组织才能满足信息安全要求，它同样应在系统建设及开发过程中起主导作用。网络的硬件系统、软件系统及开放系统互连的基本参考模型中的每层都涉及相应的安全问题。这里对安全体系结构的主要元素：安全策略、信息分级、风险评估、安全基础设施、网络隔离、常见的网络安全设备、安全服务、安全事件管理与安全管理、政策法规几个方面进行加以介绍，对要求高的部分会在相关章节做更为详细的论述。

1. 安全策略

有效的安全策略对信息网络安全是十分必要的。安全策略以一种概括的方式包含了大量的信息，它不指定所使用的技术，而是着重于描绘一种完整的安全图景。策略包含了用以达成安全目标的方法，为使用者提供行动的指导。网上的一切活动都要与安全策略保持一致。

2. 信息分级

在信息分级策略指导下对信息机密性进行分级。信息分级级别受许多因素制约，但最主要的约束是在风险和对风险的容忍度之间的权衡。通过对信息进行分级的方法评定风险并进行应付，便于采取更为高效的控制措施将风险降低到可接受的程度。

3. 风险评估

风险是构成“安全性”基础的基本概念。风险是需要保护的潜在损失，任何信息安全系统中都存在脆弱点即风险，它可以存在计算机系统和网络中或者管理过程中。脆弱点因为有风险，要评估出威胁出现后或攻击成功时系统所遭受的损失，从而衡量风险，并对风险进行管理。

4. 安全基础设施

实现网络安全需要完善的安全基础设施。依据安全策略，安全基础设施应能够确保其体

系结构中的大量组件协同使用，全面提高安全状况，使之超出任何单一组件的方式进行组织。只有协同工作的组件才能成为安全基础设施的一部分。

5. 网络隔离

网络隔离的指导思想是在保证互连互通的前提下，尽可能的安全。网络通常由一些网段组成，而不是一个大的集中式网络。采取把网络从公共的 Internet 物理隔离，可以防止来自 Internet攻击。网段间的隔离，可使管理者有能力控制那些流量可以在给定的网络上与其他网络之间进行传输。网络隔离是通过多种不同的技术或这些技术的结合来实现。网络隔离技术就是要解决目前网络安全存在的最根本问题，包括对操作系统的依赖和对 TCP/IP 协议的依赖，因为它们都有漏洞；解决通信连接的问题，因为内网和外网直接连接时，存在基于通信的攻击。内部网络通常使用防火墙(Firewall)平台进行隔离，目前也有专用的网络隔离器。

6. 常见的网络安全设备

目前，常见的网络安全设备很多，归结起来主要有防火墙、入侵检测系统(IDS)、虚拟专用网(VPN)和蜜罐(Honey pot)等。

7. 安全服务

国际标准化组织的 ISO 7498 -2 标准将五大类安全服务(身份鉴别、访问控制、数据保密、数据完整性、不可否认性)以及提供这些服务的 8 类安全机制及其相应的 OSI 安全管理置于 7 层模型之中，以实现访问控制、数字签名与身份认证以和信息加密来保障安全服务。

8. 安全事件管理与安全管理

1) 安全事件管理(SEM)

网络连接的不断增加和网络区域的不断扩展给安全事件的有效管理提出了更高的要求。成功地处理事件和无错操作的关键在于理解网络的拓扑结构(包括合理、有力的流量分析工具)，并在监控系统或中间系统上对可疑事件触发器进行记录并发出警告。必须仔细检查事件源和事件的严重性以确保数据的相关和可靠。监控系统必须能够对各种警告进行分类以便生成能够反映系统情况的可用报告，从而达成先处理关键事件的逻辑方式，同时将次要问题按照一定方式进行分类。安全事件管理包括事件收集、逻辑分组和分类、SEM 工程的规划和启动等。

2) 安全管理

安全管理主要是指管理和维护网络系统安全性的过程。安全管理对有效控制和降低风险是极为重要的，对系统安全运行起着重要作用。安全管理给整个体系结构及控制该体系结构使用的操作提供必要的指导和方向。安全管理包括事故管理、应急响应、过程管理和组件管理等。

9. 政策法规

信息系统安全是一个综合性的课题，需要法律与政策支持，对安全事件的调查处理要依据法律和政策。从体系结构的观点来看，法律法规是信息安全的所有因素中最重要的因素，只有在法律法规相对完善的前提下才可能构造合理的信息安全体系。

1.2.3 安全体系结构元素的关系

网络安全体系结构是从整体上、全局上考虑安全问题的，它需要在安全策略设计、信息安全传输、网络安全使用及安全设备间互动等方面，都能满足系统整体安全要求，而其中人的因