密码学

在信息系统安全中的研究及应用

董　仕◎著

“国家一级出版社” 中国纺织出版社 “全国百佳图书出版单位”

密码学在信息系统安全中的研究及应用

董仕 著

中国纺织出版社

图书在版编目（CIP）数据

密码学在信息系统安全中的研究及应用 / 董仕著
. -- 北京 : 中国纺织出版社, 2018.3
ISBN 978-7-5180-4308-8

Ⅰ. ①密… Ⅱ. ①董… Ⅲ. ①密码学－应用－信息系统－安全技术－研究 Ⅳ. ①TN918.1 ②TP309

中国版本图书馆CIP数据核字(2017)第282128号

责任编辑：汤　浩　　**责任印制**：储志伟

中国纺织出版社出版发行
地　　址：北京市朝阳区百子湾东里 A407 号楼　**邮政编码**：100124
销售电话：010-67004422　**传真**：010-87155801
http://www.c-textilep.com
E-mail：faxing@c-textilep.com
中国纺织出版社天猫旗舰店
官方微博 http://weibo.com/2119887771
虎彩印艺股份有限公司　各地新华书店经销
2018 年 3 月第 1 版第 1 次印刷
开　　本：880mm×1230mm　1/32　**印张**：7.5
字　　数：240 千字　**定价**：55.00 元

前 言 preface

信息网络的国际化、社会化、开放化和个人化的特点，决定了它在给人们提供高效率、高效益、高质量的“信息共享”的同时，也投下了不安全的阴影。随着政府和人民对网络环境和网络资源依赖程度的不断加深，信息泄露、黑客入侵、计算机病毒传播，甚至于威胁国家安全的问题会出现得越来越多。密码技术作为保障信息安全的核心技术，在古代就已经得到应用，但仅限于外交和军事等重要领域。目前随着现代计算机技术的飞速发展，密码技术正在不断向更多其他领域渗透。

密码技术不仅能够保证机密信息的加密，而且能够实现数字签名、身份验证、系统安全等功能。所以使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性，还可以防止信息被篡改、伪造和假冒。

网络与信息安全是一个综合、交叉的学科领域，涉及安全体系结构、安全协议、密码理论、信息分析、安全监控、应急处理等各个方面，还要利用数学、电子、信息、通信、计算机等诸多学科的长期知识积累和最新发展成果。信息安全要综合利用数学、物理、通信和计算机诸多学科的长期知识积累和最新发展成果，进行自主创新研究，加强顶层设计，提出系统的、

完整的、协同的解决方案。网络信息安全面临的威胁是多方面的，具有无边界性、突发性、蔓延性和隐蔽性等新的特点。网络模糊了地理、空间上的边界概念，使得网上的冲突和对抗更具隐蔽性。

病毒对计算机网络的攻击往往是在没有任何先兆的情况下突然发生的，而且会沿着网络迅速蔓延。对网络信息安全防御的困难还在于，一个攻击者仅需要发起一个成功的攻击，而防御者则需要考虑所有可能的攻击，而且这种攻击是在动态变化的。因此，仅从技术上解决网络信息安全是有一定风险的。国际标准化组织（ISO）将“信息安全”定义为：为数据处理系统建立和采取的技术和管理的安全保护，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。简单说，信息安全的基本属性有保密性、完整性、可用性、可靠性和可控性。信息保密性则是要确保信息不被泄露给非授权的个人和实体或供其使用。信息的保密性包括文件的保密性、传输过程中的保密性等两个方面。信息的完整性是指信息在存储或传输时不被修改、不被破坏，不被插入、不延迟、不乱序和不丢失的特性。信息可用性是指信息可被合法用户访问并能按要求顺序使用的特性。信息可控性是指授权机关可以随时控制信息的机密性。每一个用户只能访问自己被授权可以访问的信息。同时对系统中可利用的信息及资源也要进行相应的分级，确保信息的可控性。信息的可靠性是指以用户认可的质量连续服务于用户的特性。这不仅是要保护信息的安全可用，还和信息系统本身的可靠性有关。实际上不论是局域网还是广域网，都是

一种系统，所以系统安全问题的解决，必然是一项系统工程，必须采用系统工程学的方法、运用系统工程学的原理来设计网络信息安全体系。解决网络信息安全的基本策略是技术、管理和法制并举。技术是核心，要通过关键技术的突破，构筑起国家信息安全技术防范体系。管理是关键，根据“木桶原理”，信息安全链条中任何一个环节的脆弱都有可能导致安全防护体系的失效，因此，必须要加强各管理部门和有关人员间的密切合作。法制是保障，通过建立信息安全法规体系，规范信息化社会中各类主体的行为，以维持信息化社会的正常运作秩序。

网络环境下信息的保密性、完整性、可用性和抗抵赖性，都需要采用密码技术来解决。密码技术是信息安全技术的核心，它主要由密码编码技术和密码分析技术两个分支组成。密码编码技术的主要任务是寻求产生安全性高的有效密码算法和协议，以满足对消息进行加密或认证的要求。密码分析技术的主要任务是破译密码或伪造认证信息，实现窃取机密信息或进行诈骗破坏活动。这两个分支既相互对立又相互依存，正是由于这种对立统一关系，才推动了密码学自身的发展。

目前人们将密码理论与技术分成两大类，一类是基于数学的密码理论与技术，包括公钥密码、分组密码、序列密码、认证码、数字签名、Hash 函数、身份识别、密钥管理、PKI 技术、VPN 技术等；另一类是非数学的密码理论与技术，包括信息隐藏、量子密码、基于生物特征的识别理论与技术等。网络信息安全体系的构建要求我们必须合理地使用多种密码技术，这样才能保证信息的可靠性、保密性、完整性、可用性和可控性。

使用信息隐藏和公钥密码、分组密码等密码技术可保证信息的保密性。信息隐藏对于在网络中保护信息不受破坏起到重要作用，信息隐藏是把机密信息隐藏在大量信息中不让对手发觉的一种方法。主要侧重于隐写术、数字水印、潜信道、隐匿协议、可视密码等方面的理论与技术的研究。Hash 函数（也称杂凑函数或杂凑算法）就是把任意长的输入消息串变化成固定长的输出串的一种函数。Hash 函数主要用于完整性校验和提高数字签名的有效性，目前已有很多方案。这些算法都是伪随机函数，任何杂凑值都是等可能的。输出并不以可辨别的方式依赖于输入。数字签名是对电子形式的消息签名的一种方法。基于公钥密码体制和私钥密码体制都可以获得数字签名，特别是公钥密码体制的诞生为数字签名的研究和应用开辟了一条广阔的道路。关于数字签名技术的研究，目前主要集中在基于公钥密码体制的数字签名技术的研究。数字签名的研究内容非常丰富，主要有 RSA 数字签名算法、ELgaml 数字签名算法、椭圆曲线数字签名算法和有限自动机数字签名算法等。

简单地说，PKI 技术就是利用公钥理论和技术建立的提供信息安全服务的基础设施。PKI 是解决信任和加密问题的基本解决方案，本质就是实现了大规模网络中的公钥分发问题，建立了大规模网络中的信任基础。PKI 是创建、管理、存储、分发和撤销基于公钥加密的公钥证书所需要的一套硬件、软件、策略和过程的集合。PKI 为开放的 Internet 环境提供了四个基本的安全服务：

（1）认证，确认发送者和接收者的真实身份；

（2）数据完整性，确保数据在传输过程中不能被有意或无意地修改；

（3）不可抵赖性，通过验证，确保发送方不能否认其发送消息；

（4）机密性，确保数据不能被非授权的第三方访问。

另外，PKI还提供了其他的安全服务，主要包括以下两个：

（1）授权，确保发送者和接收者被授予访问数据、系统或应用程序的权力；

（2）可用性，确保合法用户能正确访问信息和资源。

VPN是利用接入服务器（Access Server）、广域网上的路由器或VPN专用设备在公用的WAN上实现虚拟专网的技术。也就是说，用户觉察不到他在利用公用WAN获得专用网的服务。如果强调其安全性，可以认为VPN是综合利用了认证和加密技术，在公共网络（比如Internet）上搭建一个只属于自己的虚拟专用安全传输网络，为关键应用的通信提供认证和数据加密等安全服务。如果将VPN的概念推广一步，我们可以认为凡是在公共网络中实现了安全通信（主要包括通信实体的身份识别和通信数据的机密性处理）的协议都可以称之为VPN协议。到目前为止，VPN已经在网络协议的多个层次上实现，从数据链路层、网络层、传输层一直到应用层。特别是IPSec标准的制定，对实施VPN奠定了坚实的基础。

我们必须正确理解密码学在网络和信息安全中的地位。密码技术仅仅是解决信息和信息系统安全的关键技术之一，单靠密码技术不能彻底解决信息和信息系统的安全问题，安全问题

涉及人、技术、管理和操作等多方面的因素。安全系统的防御等级遵循“木桶”原理，取决于其最薄弱的环节。总而言之，在解决信息和信息系统安全这个问题上，密码技术不是万能的，但离开密码技术是万万不能的。

目 录 content

第一章 信息系统安全概述

互联网的迅速发展，在极大地推动经济社会发展、方便人们生产生活的同时，也带来了大量的网络信息安全问题，为政府部门实施社会管理、维护国家安全和利益带来了新的问题和挑战。

一、信息系统安全的基本概念

（一）信息系统安全的定义

所谓信息系统安全就是依靠法律法规、道德纪律、管理细则和保护措施、物理实体安全环境、硬件系统安全措施、通信网络安全措施、软件系统安全措施等实现信息系统的数据信息安全。

（二）信息系统安全的内容

信息系统的安全包括物理安全、网络安全、网络反病毒、操作系统安全、应用软件安全、数据安全和管理安全。

（1）物理安全主要包括环境安全、设备安全、媒体安全等。

（2）网络安全主要包括内外网隔离及访问控制系统防火墙、物理隔离或逻辑隔离；内部网不同网络安全域的隔离及访问控制；网络安全测试与审计；网络防病毒和网络备份。

（3）网络反病毒主要包括预防病毒、检测病毒和消毒。

（4）其他方面的安全，如操作系统安全、应用软件安全以及数据安全和管理安全等。

网络信息安全问题缘于信息技术的迅猛发展与广泛应用，但又超出了信息技术自身的范畴，它不仅表现为对信息技术发展的强烈依赖，而且从网络信息安全概念提出之日起，就自然地表现为对物理环境、人的行为的强烈依赖。从微观角度看，国家网络信息安全是一种融合了技术层面、物理环境和人的因素等多方面的综合安全；从宏观角度看，国家网络信息安全兼具“传统安全”与“非传统安全”的特征，体现为国家对网络信息技术、信息内容、信息活动和方式以及信息基础设施的控制力。

网络信息系统安全是一种基础安全。随着社会信息化程度的日益加深，无论是人们社会生产和生活的各种活动，还是国家机关、各种企业事业组织履行社会管理、提供社会服务以及自身的正常运转，都越来越紧密地与计算机、信息网络结合在一起；无论是经济社会发展，还是国家政治外交、国防军事等活动，都越来越依赖于庞大而脆弱的计算机网络信息系统。如今，网络信息系统已经成为一切政治、经济、文化和社会活动的基础平台和神经中枢；而对于个人而言，了解并熟悉信息系统安全也有很大的意义。

信息系统安全本身包括的范围很大。大到国家军事政治等机密安全，小到如防范商业企业机密泄露、防范个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、

信息认证、数据加密等），直至安全系统，其中有任何一个安全漏洞便可以威胁全局安全。信息安全服务至少应该包括支持信息网络安全服务，以及基于新一代信息网络体系结构的网络安全服务体系结构。

信息系统安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。信息系统安全主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。

信息系统安全的根本目的就是使内部信息不受外部威胁，因此信息通常要加密。为保障信息安全，要求有信息源认证、访问控制，不能有非法软件驻留，不能有非法操作。它是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。随着时代的发展，日益繁多的事情托付给计算机来完成，敏感信息正经过脆弱的通信线路在计算机系统之间传送，信息系统的安全性就显得更重要了。

传输信息的方式很多，有局域计算机网、互联网和分布式数据库，有蜂窝式无线、分组交换式无线、卫星电视会议、电子邮件及其他各种传输技术。信息在存储、处理和交换过程中，都存在泄密或被截收、窃听、窜改和伪造的可能性。不难看出，单一的保密措施已很难保证通信和信息的安全，必须综合应用各种保密措施，即通过技术的、管理的、行政的手段，实现信源、信号、信息三个环节的保护，借以达到秘密信息安全的目的。信息安全的威胁来自方方面面，不可一一罗列。但这些威胁根据其性质，基本上可以归结为以下几个方面：（1）信息泄露：保护的信息被泄露或透露给某个非授权的实体；（2）破坏信息的完整性：数据被非授权地进行增删、修改或破坏而受到损失；（3）拒绝服务：信息使用者对信息或其他资源的合法访问被无条件地阻止；（4）非法使用（非授权访问）：某一资源被某个非授权的人，或以非授权的方式使用。

而一个完整的信息系统安全需要实现以下目标。（1）真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别；（2）保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义；（3）完整性：保证数据的一致性，防止数据被非法用户篡改；（4）可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝；（5）不可抵赖性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的；（6）可控制性：对信息的传播及内容具有控制能力；（7）可审查性：对出现的网络安全问题提供调查的依据和手段。

二、信息系统安全的对策

从根本意义上讲，绝对安全的计算机是根本不存在的，绝对安全的网络也是不可能有的。只要使用，就或多或少地存在安全问题。我们在探讨安全问题的时候，实际上是指一定程度的网络安全。一般来说，网络越安全，就越意味着对网络使用的不方便。即网络的安全性通常是以网络的开放性、便利性和灵活性为代价的。计算机信息系统安全是一个复杂的系统工程，国际上普遍认为，它不仅涉及技术、设备、人员管理等范畴，还应该依法律规范作保证，只有各方面结合起来，相互弥补，不断完善，才能有效地实现网络信息安全。从技术的角度来说，信息系统安全的对策主要有以下这几种。

（一）防火墙技术

所谓防火墙，就是在内部网与外部网之间的截面上构造一个保护层，并强制所有的连接都必须经过此保护层，在此进行检查和连接，只有被授权的通信才能通过此保护层，从而保护内部网资源免遭非法入侵。防火墙已成为实现安全策略的最有效工具之一，并被广泛应用在 Internet 上。

（二）数据加密

网络安全的另一个非常重要的手段就是加密技术。与防火墙相比，数据加密技术比较灵活，更加适用于开放网络。数据加密由行行式式的加密算法来具体实施，其实质是对以符号为基础的数据进行移位和置换的变换算法。这种变换是受称为密钥的符号串控制的。通过对网络传输的信息进行加密，信息传输在全封闭状态下运行，传输的信息不会被第三者识别、修改、