LOIS

信息安全国家重点实验室

信息安全丛书

Technologies on Public Key Infrastructure

PKI技术

荆继武　林璟锵　冯登国 编著

科学出版社
www.sciencep.com

信息安全国家重点实验室信息安全丛书

PKI 技 术

荆继武 林璟锵 冯登国 编著

国家高技术发展计划项目资助（项目编号：2006AA01Z454）

科 学 出 版 社
北 京

内 容 简 介

本书专门讲述公开密钥基础设施技术。本书是在作者多年研究经验的基础上，结合研究生专业课程的教学实践撰写而成。全书共分 15 章，主要内容包括：密码学基础、PKI 系统的基本结构、数字证书的结构与编码、目录技术、证书的生命周期、证书撤销技术、证书策略、PKI 互联技术、PKI 应用技术以及属性证书与授权技术。本书从需要解决的网络安全问题出发，逐步深入地介绍了 PKI 解决问题的先进思路和工程方法，以及 PKI 的应用与发展。为帮助读者理解书中内容，每章后附有参考文献和习题。

本书可作为高等院校计算机、通信、信息安全等专业的教学参考书，也可供从事相关专业的教学科研和工程技术人员参考。

图书在版编目(CIP)数据

PKI 技术/荆继武，林璟锵，冯登国编著. —北京：科学出版社，2008
（信息安全国家重点实验室信息安全丛书）
ISBN 978-7-03-021906-0

I. P… II.①荆…②林…③冯… III.因特网-安全技术 IV. TP393.408

中国版本图书馆 CIP 数据核字(2008)第 064898 号

责任编辑：鞠丽娜/责任校对：赵 燕
责任印制：吕春珉/封面设计：三函设计

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

铭浩彩色印装有限公司印刷

科学出版社发行 各地新华书店经销

*

2008 年 5 月第 一 版 开本：B5 (720×1000)
2008 年 5 月第一次印刷 印张：24 3/4
印数：1—4 000 字数：495 000

定价：46.00 元

（如有印装质量问题，我社负责调换〈环伟〉）
销售部电话 010-62136131 编辑部电话 010-62138978-8002

《信息安全国家重点实验室信息安全丛书》

编委会

序　言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。数字化的生存方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地，也正在以信息化带动工业化的国策引导下焕发着青春。电子政务、电子商务等各种信息化应用之花，如雨后春笋，在华夏沃土上竞相开放，炎黄子孙们在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。治水、训火、利用核能都曾经经历了多么漫长的时日。不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。但是，工具的不完善，会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性，存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾御技能不足的情况下，损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力，在信息空间也同样存在。在这个空间频频发生的有些人利用系统存在的脆弱性，运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。什么是信息安全？怎样才能保障信息安全？这些问题都是严肃的科学和技术问题。面对人机结合，非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真的研究。我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头鼠脸，自暴自弃，我们需要的是具有革命的乐观主义精神，坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的，今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的，它涉及到人、社会和技术，因此，仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看，只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段，才能取得良好的效果。

为了推动我国信息化发展的进程，信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中，我们既注重学术水平，又注意其实用价值。本丛书从信息安全保障体系，操作系统安全，数据库安全，网络安全，无线网络安全，网络攻击，密码技术，PKI 技术，信息隐藏，安全协议，安全事件应急响应，量子密码通信等多个角度，分析和总结信息安全的科学问题以及信息安全保障的理论与技术，因此，这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中，以使一些读者阅读本丛书后在理论、方法、技术上有新的启发和收获，从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的，今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言，它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们一起努力，不断地深化自己的研究，借鉴国外先进的科学技术，结合国情，与时俱进地推出信息安全保障的新理论、新办法和新手段，用我们的智慧保卫我们的信息疆土，使我们的信息家园尽量祥和安宁。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

前　言

信息安全已经成为信息化发展中不可缺少的技术基础。公钥基础设施（PKI）利用非对称密码学的优势，通过基础设施的工程理念，利用标准的接口为用户提供真实性、保密性、完整性和不可否认的安全服务。到目前为止，仍没有一种技术能够完全替代 PKI 技术来提供如此全面的安全服务。随着技术的进步，网络已经无处不在，各种网络应用不断涌现，安全要求也就越来越迫切。随着这种潮流的出现，PKI 的技术和原理已逐步地成为现代信息技术的基础。各个品牌的浏览器，各种型号的 Web 服务器，各种操作系统都支持标准的 PKI 技术。PKI 技术已经成为这些系统运行不可缺少的安全技术支撑。

市场上已经有多种涉及 PKI 的书，也有专门论述 PKI 的著作，但现有的著作多是基于国际标准，注重实施方法和标准的描述，而本书则更注重对 PKI 技术的原理上的描述。希望读者通过阅读本书，不仅能够懂得 PKI 技术本身，更能够在现有的技术标准基础上，理解和发现符合 PKI 基本原理的新的技术和方法，更好地做到触类旁通。本书的内容不仅包括了需要知道的概念和设计实施方法，如国际标准中的基本内容。更重要的，本书包括很多有关基本原理的内容，对 PKI 的这些深入理解是作者在这方面多年研究的结果。由于 PKI 正在发展中，只有理解了 PKI 中的诸多的为什么，才能更加正确地规划、设计符合新的网络环境的 PKI 体系，开发、维护和管理以新的 PKI 为安全基础的新的网络信息系统。

本书首先通过综述给读者提供了一个关于 PKI 的总体映像，通过密码学基础章节为那些没有密码学基础的读者提供了必要的密码学基础知识。随后，本书从非对称密码学应用入手，引入了 PKI 的基本结构，介绍了 PKI 中最重要的元素——证书的基本结构与编码。紧接着的章节就开始介绍 PKI 的核心技术，包括 PKI 用到的目录以及与证书的生命周期相关的概念和方法。核心的概念介绍完成后就以工程中的实施技术为主，介绍证书撤销的服务技术以及建立 CA 和应用 PKI 必须了解的证书策略与认证业务声明。然后，本书站在一个更为宏观的视角上介绍为保密监控和密文恢复必须采用的双证书体系，以及为更大范围的互操作所必须的 PKI 互联技术。根据前面的结果，本书对证书和 CRL 扩展进行了总结。本书还介绍了 PKI 应用的相关问题，包括：PKI 的实体身份鉴别技术、应用系统技术以及利用 PKI 以及属性证书的授权相关技术，最后介绍了在 PKI 技术研究领域的最新进展。

本书是在信息安全国家重点实验室认证授权课题组完成的“公开密钥基础设

施技术研究与应用”这一重点课题的研究成果的基础上撰写而成的。该研究成果获得 2005 年国家科技进步二等奖。该书的写作还得到了国家高技术发展计划项目的资助（项目编号：2006AA01Z454）。在本书的撰写过程中，夏鲁宁、文晓阳、张楠、马存庆、刘琦、查达仁、徐晨亮和王晶参加了校对、录入、绘图等工作，在此表示感谢。

特别感谢科学出版社的鞠丽娜老师在百忙中为本书提供了许多编写和修改建议，使得本书更加具有可读性和系统性。

由于作者水平所限，书中难免存在不妥之处，恳请读者批评指正。

作　者

2008 年 2 月

目　录