<<PKI技术>>

图书基本信息

书名：<<PKI技术>>

13位ISBN编号：9787030219060

10位ISBN编号：7030219066

出版时间：2008-5

出版时间：科学出版社

作者：荆继锵，林Z锵，冯登国　编著

页数：375

前言

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，社会上和国标间存在着竞争、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。

<<PKI技术>>

内容概要

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。

<<PKI技术>>

书籍目录

章节摘录

插图：美国国家审计总署在2001年和2003年的报告中都把PKI定义为由硬件、软件、策略和人构成的系统，当完善实施后，能够为敏感通信和交易提供一套信息安全保障，包括保密性、完整性、真实性和不可否认性.尽管这个定义没有提到公开密钥技术，但到目前为止，满足上述条件的也只有公钥技术构成的基础设施。
也就是说，只有第一个定义描述的基础设施才符合这个PKI的定义。
所以这个定义与第一个定义并不矛盾.综上所述，我们认为：PKI是用公钥概念和技术实施的，支持公开密钥的管理并提供真实性、保密性、完整性以及可追究性安全服务的具有普适性的安全基础设施。
1.2 PKI的目标PKI就是一种基础设施，其目标就是要充分利用公钥密码学的理论基础，建立起一种普遍适用的基础设施，为各种网络应用提供全面的安全服务。
公开密钥密码为我们提供了一种非对称性质，使得安全的数字签名和开放的签名验证成为可能。
而这种优秀技术的使用却面临着理解困难、实施难度大等问题。
正如让每个人自己开发和维护发电厂有一定的难度一样，要让每一个开发者完全正确地理解和实施基于公开密钥密码的安全系统有一定的难度。
PKI希望通过一种专业的基础设施的开发，让网络应用系统的开发人员从繁琐的密码技术中解脱出来而同时享有完善的安全服务。
将PKI在网络信息空间的地位与电力基础设施在工业生活中的地位进行类比可以更好地理解PKI.电力基础设施，通过伸到用户的标准插座为用户提供能源，而PKI通过延伸到用户本地的接口，为各种应用提供安全的服务。
有了PKI，安全应用程序的开发者可以不用再关心那些复杂的数学运算和模型，而直接按照标准使用一种插座（接口）.正如电冰箱的开发者不用关心发电机的原理和构造一样，只要开发出符合电力基础设施接口标准的应用设备，就可以享受基础设施提供的能源。
PKI与应用的分离也是PKI作为基础设施的重要标志。
正如电力基础设施与电器的分离一样。
网络应用与安全基础设施实现分离，有利于网络应用更快地发展，也有利于安全基础设施更好地建设.正是由于PKI与其他应用能够很好地分离，才使我们能够将其称为基础设施，PKI也才能从千差万别的安全应用中独立出来，才能有效地独立地发展壮大。

编辑推荐

《信息安全国家重点实验室信息安全丛书·PKI技术》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。

版权说明