RSA PRESS

[美] Andrew Nash
William Duane
Celia Joseph
Derek Brink 著

张玉清 陈建奇 杨 波 薛 伟 等译

PKI

Implementing and Managing E-Security

公钥基础设施(PKI)实现和管理电子安全

有效地规划和实施PKI技术

保护系统和安全的在线交易

通过案例研究并遵循逐步实现技术进行学习

McGraw Hill

清华大学出版社

公钥基础设施(PKI)

实现和管理电子安全

[美] Andrew Nash
William Duane
Celia Joseph
Derek Brink 著

张玉清 陈建奇 杨 波 薛 伟 等译

清华大学出版社

(京)新登字 158 号

公钥基础设施(PKI)：实现和管理电子安全
Andrew Nash/William Duane/Celia Joseph/Derek Brink：PKI：Implementing and Managing E-Security
EISBN：0-07-213123-3

北京市版权局著作权合同登记号　图字 01-2001-3172 号

图书在版编目(CIP)数据

公钥基础设施(PKI)：实现和管理电子安全/(美)那什等著；张玉清等译. —北京：清华大学出版社，2002
书名原文：PKI：Implementing and Managing E-Security
ISBN 7-302-05616-1

Ⅰ. 公…　Ⅱ. ①那… ②张…　Ⅲ. 计算机网络－安全技术　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2002)第 105347 号

出 版 者：清华大学出版社(北京清华大学学研大厦，邮编 100084)
http://www.tup.tsinghua.edu.cn
责任编辑：赵彤伟　汤斌浩
印 刷 者：北京牛山世兴印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×960 1/16　**印张**：27.25　**字数**：544 千字
版　　次：2002 年 12 月第 1 版　2002 年 12 月第 1 次印刷
书　　号：ISBN 7-302-05616-1/TP・3311
印　　数：0001～4000
定　　价：56.00 元

译者序

为解决因特网的安全问题，世界各国进行了多年的研究，初步形成了一套比较成熟和完善的因特网安全解决方案——公钥基础设施(Public Key Infrastructure，PKI)。PKI 技术采用证书管理公钥，通过第三方可信任机构——证书机构(Certificate Authority，CA)，把用户的公钥和用户的其他标识信息(如名称、电子邮件地址、身份证号等)捆绑在一起，从而在因特网上验证用户的身份。

目前，安全的电子商务就是采用建立在 PKI 基础上的数字证书，通过对要传输的数字信息进行加密和签名来保证信息传输的机密性、真实性、完整性和不可否认性(又称非否认性)，从而保证信息的安全传输和交易的顺利进行。PKI 已成为电子商务应用系统、乃至电子政务系统等网络应用的安全基础和根本保障。

从发展趋势来看，随着因特网应用的不断普及和深入，政府部门需要 PKI 支持管理；商业企业内部、企业与企业之间、区域性服务网络、电子商务网站等都需要 PKI 技术和解决方案。

在这种情况下，我们开始了清华大学校园网 PKI 系统的研究和建设。清华大学校园网经过多年的建设，已形成了一个规模庞大的国内领先和国际先进的大学校园网。随着校园网的深入建设和校园内网络的广泛普及和应用，网络与信息安全的要求和保障已成为校园网建设的核心课题之一，尤其是清华大学校园网建设的“5A”工程(任何人、任何地方、任何时间、任何平台和任何服务)更是对安全提出了高要求。从国内外发展趋势和清华大学的现状出发，我们规划和建设了清华大学校园网 PKI 系统，为建成数字校园打下了坚实和完善的安全基础。

在研究和建设清华大学校园网 PKI 系统的过程中，我们发现国内介绍 PKI 系统的书籍较为缺乏，一些书籍主要是以知识性和概念性的介绍居多，不能完全满足用户对 PKI 技术的深入了解。为此，我们组织翻译了这本美国 RSA Press 出版的《公钥基础设施(PKI)：实现和管理电子安全》一书。该书第一作者是美国 RSA 信息安全公司的 PKI 标准和技术方面的负责人，其余几位也都是顶级的专家和

技术行家。作者从 PKI 基础知识出发,深入浅出地描述了 PKI 系统部件和组成,尤其是从技术层面剖析了 PKI 的实现技术和系统架构,这对用户了解、研发、建设和应用 PKI 来说都是一本不可多得的好书。我们阅读后,获益匪浅,在此郑重向读者推荐这本 PKI 方面的权威著作。

参加本书翻译的人员有:张玉清、陈建奇、杨波、王春玲、薛伟、王思锋和曹爱玲等;审校人员有:张玉清和陈建奇;全书由张玉清统稿。由于时间和能力有限,难以做到尽善尽美,不当之处在所难免,恳请读者批评指正。联系我们的 e-mail 为:zhangyq@ChinaCrypt.net。

译 者

2001 年 8 月于清华园

前　言

PKI：实现和管理电子安全

如果你曾经在 Web 上开展过电子商务，那么很有可能曾经和一些 Web 站点进行过安全的数据交换——例如你的名字、口令、信用卡号码、订单信息等——所有这些信息都是通过 Internet 安全传送的，它们都用你的计算机和那个 Web 站点之间共享的一个密钥加了密，这样其他人就不能读取这些信息了。

这个密钥是如何得到的呢？

除非你的计算机针对每一个你可能要访问的 Web 站点都预装了一个秘密密钥（然而你的计算机并没有这么做），或者至少预装了访问某个中心密钥服务器的秘密密钥（然而中心密钥服务器不止一个），否则你就需要利用某种方式和该 Web 站点建立这个共享的秘密密钥。你的计算机不能发送这个秘密密钥，否则其他人就有可能截获它。你的计算机和该 Web 站点需要以某种方式，通过报文交换最终得到那个秘密密钥，这种方式应该能够确保别人无法计算出这个秘密密钥——这看起来相当困难，因为在你的计算机和该 Web 站点之间事先没有任何共享秘密。

25 年以前，学术界的科学家们有了非凡的发现，他们发现无须共享任何秘密就可以加密报文，而从事保密斗争的研究者早在 30 年前就发现了这一点。他们指出，和传统的使用同一个（same）密钥进行加密和解密的方式不同，可以用一个密钥加密而用另外一个不同的密钥解密。那个加密密钥可以公开，就像电话号码一样。而那个解密密钥要保持私有，就像电话一样。任何人都可以打电话给你，（但愿）只有你能够接电话。

这一发现被称为公钥密码学（Public Key Cryptography，PKC），它回答了你的计算机如何同一个 Web 站点建立共享秘密密钥的问题。实际上，你的计算机会查找该 Web 站点的公开加密密钥，并且用该公钥加密一个随机生成的秘密密钥。该 Web 站点随后用它的私有解密密钥对上述数据进行解密，恢复出你的计算机所生成的那

个秘密密钥。你的其余报文就用这个共享的秘密密钥进行加密。

然而,还有一个本质的问题:你的计算机如何知道它查找的正是该 Web 站点的公钥而不是别人的?(想象一下,在电话簿上你的名字之后列了别人的电话号码该怎么办?)这就是公钥基础设施(Public Key Infrastructure,PKI)所要解决的问题,那就是匹配公钥和其拥有者。

公钥密码学是其中容易的部分。而公钥基础设施,或者说 PKI,是我们今天所面临的挑战。就像电话号码一样,人们的公钥偶尔也会变化;而且就像电话号码簿一样,有许多公钥发布者,它们分别服务于不同的社群和不同的用途。应该信任哪一个发布者,用于何种用途?如果一个发布者不再被信任了怎么办?如何知道某人的公钥是否仍然正确?随着数字签名这一 PKI 的主要应用越来越普及,所有这些问题也就变得特别地重要。

本书将引导你了解 PKI 涉及的基本构件和主要问题、需要解决的问题以及可用的解决方案。作者务实、平易的介绍方式使得本书对 PKI 的介绍既意味深长又通俗易懂——这一切都得益于多年来从事计算机网络技术规划和设计所取得的经验。我们希望你会喜欢这本书——希望下一次当你通过因特网安全地发送用共享密钥加密的数据时,能确切地知道密钥是怎么得到的以及诸如此类的更多内容。

Scott T. Schnell
Senior Vice President of Marketing & Corporate Development
RSA Security Inc.

作者简介

Andrew Nash 是 RSA Security 公司在 PKI 标准和技术方面的负责人。他是 Keon 高级 PKI 产品系列的设计师之一，还担任 PKI 论坛技术工作组的联合主席。

William Duane 是 RSA Security 公司的一位技术负责人。他是 RSA 公司的 Keon PKI 解决方案的设计师之一，并且专门负责处理新形式的令牌部件，包括智能卡和即将出现的密码设备。

Celia Joseph 是 RSA 公司专业服务部的首席咨询工程师，负责建立和实施企业级安全解决方案。她是 RSA 公司安全评估和设计服务部门的主要顾问，她在 RSA 公司中的定制开发工作的重点是密码技术和 PKI。

Derek Brink 是 RSA 公司产品营销部的一名负责人。他的工作是为公司的公钥基础设施、认证、服务以及入侵检测产品进行市场和竞争分析、战略规划以及市场营销。他还主管 PKI 论坛执行版。

评阅者简介

作为一百多年以来一直在业界处于领先地位的技术书籍出版商，McGraw-Hill 公司在带给你最新和最具权威性的信息的同时也给自己带来了荣誉。为了确保我们的书籍满足具有最高准确性的要求，我们邀请了一些顶级的专家和技术行家对你即将要阅读的内容的准确性进行了审查。

我们很荣幸地在这里感谢下列评阅者，感谢他们的评阅：

Brian Breton，他目前是 RSA Security 公司的资深产品营销经理，负责 RSA Keon，RSA 公钥基础设施产品套件的营销。Brain 有超过 15 年的在提供 PKI、DEC 授权、Kerberos、系统安全审计以及操作系统等方面产品的公司中从事工程、产品管理以及产品营销方面工作的行业经验。

John Linn，RSA 实验室的主要工程师，从 1980 年至今一直从事网络、分布式系统和通信领域的安全技术研究。他是 Internet 工程任务组（Internet Engineering Task Force，IETF）安全部分工作的积极参与者和工作组主席，他已经在安全技术的多个方面，包括安全服务接口、信息的密码保护、分布式认证以及属性证书等方面，撰写了数篇 Internet 标准规范和会议论文。

Kathrin Winkler 有超过 20 年的从事网络软件分析、设计和工程开发工作的经验。她曾担任 Renaissance Worldwide 的主要顾问和工业分析家，还曾担任数字设备公司的网络与 Windows NT 工程组的软件咨询工程师。Winkler 女士目前是负责 Practicity 公司工程方面工作的副总裁，此公司是一家知识管理应用软件的提供商。

序

公钥基础设施(PKI)是一个极为激动人心的工作领域。它使得许多用于建立电子商务解决方案的新技术得以实现。

我们有必要全面地考察目前 PKI 发展的状况。它在许多方面都非常类似于 20 世纪 80 年代早期网络基础设施所处的状态。这也就是说,目前这个领域不断有新的发展,人们不断提出使用该技术的新方法。富有创造力的工程师、产品开发者和实现者在提出解决方案的时候有很多方法可以选择。

PKI 之所以成为技术专家感兴趣的东西,是因为尽管现在已经可以利用它做许多非常酷的事情了,但是它仍然是不完善的。PKI 的许多方面还很粗糙,还有许多问题需要解决——就像网络基础设施一样,要花许多年的时间来解决它的可用性问题。这应该不会使任何人对使用 PKI 感到泄气,因为它现在已经是一个可行的解决方案了,而且还在不断进步。

"实用的 PKI"是我(Andrew)过去说过的最受欢迎的言论之一。它介绍了 PKI 的价值,然而我却花了许多时间来指出人们没有察觉到的 PKI 的问题。这样的问题如"你怎么知道那个用公钥对事务签字的人的真实身份?""用于保存私钥的存储到底有多安全?""如果你的密钥被保存在某个 Web 浏览器的密钥存储中,那么你如何支持移动用户?"等。有许多问题是购买 PKI 产品的人们需要知道的——当然,我们提供了处理这些问题的产品(如果我只谈不能解决的问题,那么产品经理们早就非常讨厌我了)。

在此书出版之际,我得承认存在的问题比我可以谈的问题要多。之所以没有列出这些问题是因为,在人们能够理解潜在的问题之前,需要花大量的时间来建立对环境的描述,人们不会欣赏这种方式的。有太多的直接问题,无法一一处理。

今天,许多我过去提到的问题正越来越广泛地被看作 PKI 解决方案所要解决的问题。许多厂商都提供了针对这些问题的解决方案。早期的专有解决方案正不断让位给那些基于越来越多的经过验证的标准的实现。互操作性问题正在世界各地的测试实验室中被不

断地解决。PKI 论坛(www. PKIForum. org)这样的组织创造了让 PKI 厂商、顾客、用户以及实现者一起来解决 PKI 实施问题的机会。

在 PKI 及其相关领域中还在不断地出现新的机会。属性证书和特权管理基础设施正在解决对用户进行授权(在利用 PKI 确定其身份之后)和以标准方式传达访问系统的权限的问题。无线设备和那些需要在保证事务处理机密性的同时辨认大量具有高度移动性的用户群体的服务在公钥及其相关的基础设施当中找到了支撑。

我们似乎已经走过了与 PKI 相关的广告多于实际内容的阶段。现在,有趣的部分开始了——我们可以消除用户操作的复杂性,使 PKI 成为一个"真正有用的"基础设施。

本书的目的是介绍密码学和 PKI 的概念和技术,展示如何实施和使用 PKI 以支持电子商务和信息传递的迅速扩展。与此同时,还介绍了 PKI 和其他重要的安全技术,如认证鉴别技术的关系,并且处理了一些实际问题,例如如何从对 PKI 的投资中获取经济上的回报。

祝你阅读愉快!

目　录