<<互联网公钥基础设施概论>>

图书基本信息

书名：<<互联网公钥基础设施概论>>

13位ISBN编号：9787115110596

10位ISBN编号：711511059X

出版时间：2003-3

出版时间：人民邮电出版社

作者：贝南塔

译者：张千里

前言

现代密钥密码学的基础在于密钥的安全性。
这一性质并非刻意所求，而只是客观条件的限制。
考虑特定的密码算法是如何进行保密的，首先，可以对算法进行保密：如果不能对算法进行技术分析，那么算法就可以隐藏它的弱点，这样就奉行了那个不受好评.的原则——不公开即安全。
可是，没有办法能够把一个密码算法的弱点或优点永远隐藏下去，迟早一些人会通过逆向工程得到软件或硬件密码模块中的处理流程。
这一结果可能就会宣告这一算法的末日来临。
密钥算法中，密钥需要发布给通信参与者，可是，密钥发布的次数越多，安全性能就越有可能会被损害。
长期密钥的发布，违背了密钥密码学（也称作对称密钥密码学）的核心假定。
密钥的传输需要建立安全通道，虽然可以由人来亲自传输，但是这不能满足大规模分布计算的需要。
而在线发布需要高度安全的秘密通道，这样，就产生了如何启动密钥发布这一难题。
为了缓解密钥分发问题，就自然产生了密钥发布中心（KDC）的概念。
这一实体为所有其他实体所信赖，它有两个作用，一方面用来保存长期密钥，另一方面用来发布两个实体通信时所需的短期会话密钥。
后者常常还伴随有介绍一个实体给另一个实体的功能，这一般通过使用长期密钥在每个相应的实体和第三方建立的可信通道来实现。
尽管这一方法已经成为了最优秀的第三方密钥发布方案，但它缺少在互联网络这一普遍存在的计算模式下应用所需要的的灵活性。
回到我们的主题，来讨论公钥密码学的概念，公钥密码学这一概念的历史要比KDC的历史长得多。
公钥密码学的基本然而影响深远的概念是，密钥成了相关的一对：公钥和私钥。
私钥由所有者安全保护，而公钥则可以自由散播。
它的基本假设在于，知道公钥之后计算私钥，在计算上是不可能实现的。
用公钥加密的数据只能够用私钥解开。
有了这样一个吸引人的性质，公钥密码学看起来最终解决了安全密钥分发问题。
有赖于一些密钥交换机制，如Diffie-Hellman，它确实做到了这一点。
而且，公钥密码学不仅能够用于密钥交换协议，它还可以提供各种安全服务，如数字证书、抗抵赖服务以及利用那些著名的公钥算法（如RSA）进行数据加密。
自由发布公钥的前提，就是信任的建立。
基于公钥密码学的安全服务，也要依赖一种信任：即某个特定公钥确实属于它的合法所有者。
为了建立信任机制，一个很有前途的方法是利用X.509所提供的数字证书，它已被采纳为互联网络标准。
本书将试图全面介绍互联网络公钥认证方面的各个主要方面。

<<互联网公钥基础设施概论>>

内容概要

《互联网公钥基础设施概论》围绕互联网络公钥基础设施（PKI）的建立进行了广泛的讨论，介绍了密钥密码学和公钥密码学的发展历史和相关知识，并围绕着密钥分发这一问题，探讨了PKI引入的必要性。
全书重点集中在解答有关PKI部署、运行和管理中的一些最重要的问题，这些问题包括：密钥密码学和公钥密码学的基本原理；密钥分发问题以及公钥保障系统的重要地位；用PKIX来建设安全互联网系统；了解PKIX标记语言、数据编码机制以及拓扑；如何实现有效的PKI信任模型；利用LDAP作为PKIX在互联网中的存储库；证书鉴定、凭证管理，以及密钥更新等。

《互联网公钥基础设施概论》内容深入浅出，比较适合那些希望总体了解公钥基础设施与网络安全的电子商务、电子政务管理人员和技术人员阅读，对于那些已经对公钥基础设施有所了解的信息安全工程技术人员和开发人员来说，《互联网公钥基础设施概论》也不失为一本优秀的综合手册。

<<互联网公钥基础设施概论>>

作者简介

作者：（美国）贝南塔（Messaoud Benantar） 译者：张千里 等贝南塔（Messaoud Benantar），博士，高级软件工程师，工作单位是位于美国德克萨斯州奥斯汀的IBM公司。
毕业于美国纽约州Troy的轮塞拉尔（Rensselaer）工学院计算机系，并获得博士学位。
有超过10年的在各个平台上开发安全软件的经验，持有多项关于分布式系统安全的美国专利。
研究兴趣包括：系统和网络安全以及所有与互联网络计算相关的课题。

<<互联网公钥基础设施概论>>

书籍目录

章节摘录

插图：本章着眼于密钥管理评测。
密钥加密的固有性质要求密钥发布给各个相关方，以便一端加密的报文可以被对方解开。
随着所涉及的团体的增加、本地安全方针范围的变大、所引入通信方式的增多，密钥的安全发布和管理问题将变得越来越复杂。
一般说来，通过密钥密码学系统提供的安全服务要求密钥在此服务使用之前发布给两个或更多的实体。
密钥发布过程也称作密钥的建立过程。
为了抵抗潜在的窃听威胁，这个过程通常要求无论是在线还是带外来进行发布，必须通过一定的安全方式来进行。
在发布之后，密钥的长期使用使安全管理过程变得必要。
显然，密钥在本地或网络上的存储介质中必须受保护；在进一步地向远端发布的过程中，密钥传输也应当受到保护。
构建和维护密钥共享关系是同等重要的，该关系是由用户团体采用的通信方式所决定的。
例如，额外的密钥管理细节可能要求两个实体间的密钥建立过程后还要进行密码学确认。
密钥管理过程也需要支持万一密钥泄漏，在实施相应处理措施的同时，还可以更新旧的密钥。
这些密钥管理功能的复杂性是与本地所采取的策略类型相对应的。
更重要的是，它们更多取决于特定团体所遵从的模式或通信间的模式。
本章中，我们详细阐述了支持这一论断的密钥关系拓扑。
假设有，1个人为了建立一个他们内部间加密通信的渠道，他们决定使用对称加密法。
密钥建立的不同过程可能导致密钥发布的不同情形，一共有4种情形。
1.对于所有用户共用一个密钥在这种情形下，所有用户共用一个密钥并用它来对要交换的信息进行加密和解密。
这一共享的密钥需要有，z次发布，每个用户需要管理一个密钥。
这个密钥只要一处泄漏，就会导致这个群体中所有的加密通信被破解。
而且由于所有人共享一个密钥，很难可靠地实现源认证，群体中的成员可以冒充其他人的身份。
在这种情形下，非抵赖服务就无法完成。
如图2.1 所示，即为所有成员共享一个密码的情形。

编辑推荐

《互联网公钥基础设施概论》：IT先锋系列丛书

<<互联网公钥基础设施概论>>

版权说明