《网络安全管理员》

图书基本信息

书名：《网络安全管理员》

13位ISBN编号：9787111391128

10位ISBN编号：7111391128

出版时间：2012-8

出版社：程庆梅、 徐雪鹏 机械工业出版社 (2012-08出版)

页数：116

《网络安全管理员》

内容概要

《网络安全管理员》

书籍目录

《网络安全管理员》

章节摘录

版权页： 插图： 现代密码技术发展至今20余年，出现了许多高强度的密码算法和密钥管理技术。数据安全技术也已由传统的只注重保密性转移到了保密性、真实性、完整性和可控性的完美结合，并且相继发展了身份认证、消息确认和数字签名技术。 所谓加密（Encryption）是指将一个信息（或称明文——Plaintext）经过加密钥匙（Encrypt-ion Key）及加密函数转换变成无意义的密文（Ciphertext），而接收方则将此密文经过解密函数、解密钥匙（Decrypt on Key）还原成明文。这一概念是密码学的基础。 数据加密技术要求只有在指定的用户或网络下才能解除密码而获得原来的数据，这就需要给数据发送方和接收方一些特殊的信息用于加、解密，这就是所谓的密钥。需要保护的原始信息称为明文，用密钥编码操作后得到的看上去没有意义的结果称为密文。加密的优点是即使其他的控制机制（如密码、文件权限等）受到了攻击，入侵者窃取的数据仍是无用的。 密码技术的基本任务是使通常称为Alice和Bob的两个人在不安全的信道上进行通信，而他们的敌人Oscar不能理解他们正在通信的内容。 Alice打算发送给Bob的消息，我们称为明文。明文的形式可以是任意的，在计算机领域里通常是二进制数据。Alice用预先确定的密钥处理（加密）明文，得到密文，通过信道发送给Bob。在信道上通过截听而能看到密文的Oscar由于不知道解密密钥，所以不能确定明文是什么，而知道解密密钥的Bob却能解密密文得到明文。 信息加密过程是由形形色色的加密算法具体实施的，密码设计的基本公理和前提是算法公开，系统的安全性仅依赖于密钥的保密性。按照密钥使用方式不同来区分，可以将这些加密算法分为对称密钥密码算法（又称私有密钥算法）和非对称密钥密码算法（又称公钥密码算法）。两种密码体制各有优缺点，适用于不同的加密需求和应用场合。 对于加密文件，一个常被讨论但又经常被误解的内容是加密强度。什么构成了加密的强度，哪种级别的加密强度是被不同的安全需要所要求的，如何确定加密的有效强度？加密强度主要取决于3个因素：1）算法的强度。除了尝试所有可能的密钥组合之外，任何数学方法都不能使信息被解密；应该使用工业标准的算法，因为它们已经被加密学专家测试过无数次：任何一个新的或个体的方法在被商业认证之前都不被信任。 2）密钥的保密性。数据的保密程度直接与密钥的保密程度相关，算法不需要保密，被加密的数据首先与密钥共同使用，然后通过加密算法加密。 3）密钥强度。根据加密和解密的应用程序，密钥的长度是由bit为单位。在密钥的长度加上一位则相当于把可能的密钥的总数乘以2，简单地说构成一个任意给定长度的密钥的位的可能的密钥个数可以被表示为2n，因此一个40位密钥长度的算法将是240个可能的不同的密钥。

《网络安全管理员》

编辑推荐

《网络安全管理员》

版权说明