<<信息系统安全理论与技术>>

图书基本信息

书名：<<信息系统安全理论与技术>>

13位ISBN编号：9787040233490

10位ISBN编号：7040233495

出版时间：2008-3

出版时间：高等教育

作者：方勇

页数：371

<<信息系统安全理论与技术>>

内容概要

《高等学校信息安全系列教材：信息系统安全理论与技术》通过对信息系统安全的五大安全服务和多种实现机制给出比较完整而系统的介绍，使读者能系统地了解并掌握信息系统安全体系的构建方法、信息系统安全框架及其实现机制的主要内容。

<<信息系统安全理论与技术>>

书籍目录

章节摘录

版权页： 插图： 1.加密机制 加密机制是各种安全服务和其他许多安全机制的基础，既能为数据提供机密性，也能为通信业务流信息提供机密性，并且还成为本节所述其他安全服务和安全机制中的一部分，能起到支持或补充作用。
（1）加密层的选取 大多数应用将不要求在多个层上加密，加密层的选取主要取决于以下几个因素：
①如果要求全通信业务流具有机密性，可选取物理层加密或传输安全手段（例如适当的扩频技术）。
足够的物理安全、可信任的路由选择以及在中继上的类似机制能够满足所有的机密性要求。
②如果要求细粒度的保护（例如对每个应用提供不同的密钥）、抗抵赖或选择字段的保护，可选取表示层加密。
由于加密算法会耗费大量的处理能力，因此选择字段的保护是很重要的。
在表示层中的加密能提供不带恢复的完整性、抗抵赖以及所有的机密性保护。
③如果希望的是所有端系统到端系统通信的机密性保护，或者希望有一个外部的加密设备（例如为了给算法和密钥以物理保护或防止错误软件），可选取网络层加密。
它能够提供机密性与不带恢复的完整性。
虽然在网络层不提供恢复，但传输层正常的恢复机制能够用来恢复网络层检测到的攻击。
④如果要求带恢复的完整性，同时又具有细粒度保护，可选取传输层加密，它能够提供机密性、带恢复的完整性或不带恢复的完整性。
⑤对于今后的实施，不推荐在数据链路层上加密。
当关系到这些主要因素中的两项或多项时，可能需要在多个层上提供加密。
（2）加密算法的类别 加密算法可以是可逆的，也可以是不可逆的。
可逆加密算法有两大类：①对称密码体制：知道了加密密钥也就意味着知道了解密密钥，反之亦然。
②非对称密码体制：知道了加密密钥并不意味着也知道解密密钥，反之亦然。
这种系统的这两个密钥有时被称为“公钥”与“私钥”。
不可逆加密算法可以使用密钥，也可以不使用密钥。
若使用密钥，该密钥可以是公开的，也可以是秘密的。
（3）密钥管理 除了某些不可逆加密算法的情况外，加密机制的存在意味着要使用密钥管理机制。
密钥管理涉及各个不同的阶段，其中包括密钥产生、密钥分配、密钥销毁、密钥取消等。

编辑推荐

版权说明