<<信息安全工程>>

图书基本信息

书名：<<信息安全工程>>

13位ISBN编号：9787560624327

10位ISBN编号：7560624324

出版时间：2010-9

出版时间：李晖、庞辽军、裴庆祺、 李慧贤 西安电子科技大学出版社 (2010-09出版)

作者：李晖 等 著

页数：406

<<信息安全工程>>

内容概要

《信息安全工程》由庞辽军、裴庆祺、李慧贤主编，并以信息安全理论为基础，以实际工程应用为目标，有针对性、有选择性地介绍了已经被普遍应用且实用有效的安全算法、协议和系统，并给出了一些实际工程应用中积累的经验和教训。

《信息安全工程》首先介绍了当前信息安全的概念及其内涵和外延、信息安全的框架模型和安全需求、信息安全的相关技术等；然后介绍了当前解决信息安全问题常用的一些策略和实用技术，如密码算法、PKI技术、完整性技术、信息隐藏技术、生物认证技术等；接着结合系统工程方法，介绍了信息安全标准状况和现有的安全模型；最后给出了国内外解决信息安全问题的一些成功案例，包括WLAN、WMAN和WSN安全技术及WAPI方案等。

《信息安全工程》的特点是：以工程应用为载体，融理论于工程；借助于流行的安全系统，而不是孤立地介绍各种安全算法。

《信息安全工程》可作为高等院校相关专业的本科生教材，也可作为相关专业的研究生教材，同时还可作为从事网络与信息安全技术工作的广大科技人员的参考书。

<<信息安全工程>>

书籍目录

章节摘录

版权页：插图：1.密钥的产生和分配在密钥的产生过程中，关键是随机性，要求尽可能用客观的、物理的方法产生密钥，并尽可能用完备的统计方法检验密钥的随机性，使不随机的密钥序列的出现概率能够最小。
密钥的分配是密钥管理中最大的问题。
密钥必须通过最安全的信道进行分配，指派非常可靠的信使携带密钥来分配给互相通信的各用户的人工方式不再适用，因为随着用户的增多和通信量的增大，密钥更换十分频繁（密钥必须定期更换才能做到安全可靠），所以密钥在网内的自动分配方法便应运而生。
在网内，密钥可在用户之间直接实现分配，也可通过密钥分配中心（KDC，KeyDistributionCenter）分配。
用户甲向密钥分配中心发送明文，说明想和用户乙通信，也就是向KDC申请会话时使用的会话密钥。
KDC收到申请后，从用户专用的主密钥文件中找出用户甲和乙的主密钥，同时产生甲和乙通信所用的会话密钥，分别用甲、乙的主密钥加密会话密钥并发送给甲、乙双方，甲和乙即可用会话密钥进行保密通信。
KDC可以为每对用户在每次通信时产生一个新的会话密钥，这就使得破译密文变得十分困难。
主密钥是用来保护会话密钥的，因此主密钥也不能在不进行更换的情况下长期使用。
2.密钥的注入密钥的注入可采用键盘、软盘、磁卡、磁条、智能卡、USB.Key、专用设备等方式。
对密钥的注入应予以严格保护，注入过程应在一个封闭的、保密的环境，注入人员应当可靠。
操作时，只有在输入合法的口令后才可开始注入，重要的密钥应当由多人、多批次分开注入完成，不允许存在任何可能导出密钥的残留信息，一旦窃取者试图读出或分析推算出注入的密钥，密钥就会自行销毁。
3.密钥的存储与销毁在密钥产生以后，需要以密文形式存储密钥。
密钥的存储方法有两种：一种是让密钥存储在密码装置中，这种方法需大量存储和频繁更换密钥，实际操作过程十分繁琐；另一种方法是运用一个主密钥来保护其他密钥，这种方法可将主密钥存储在密码装置中，而将数量相当多的数据加密密钥存储在限制访问权限的密钥表中，从而既保证了密钥的安全性与保密性，又有利于密钥的管理。
此外，在密钥的存储过程中，加、解密的操作口令应由密码操作人员掌握；加密设备应有物理保护措施，如失电保护等；非法使用加密设施时应有审核手段；采用软件加密形式时，应有软件保护措施。
对使用时间过长或已经失效的密钥，应及时销毁。

<<信息安全工程>>

编辑推荐

《信息安全工程》：高等学校电子与通信类专业规划教材

<<信息安全工程>>

版权说明