<<信息安全概论>>

图书基本信息

书名：<<信息安全概论>>

13位ISBN编号：9787563514861

10位ISBN编号：7563514864

出版时间：2007-9

出版时间：北京邮电大学

作者：牛少彰，崔宝江，

页数：255

字数：370000

<<信息安全概论>>

内容概要

本书在第1版的基础上进行了修改和完善，并补充了一些信息安全近几年的研究成果，全书内容更加翔实和新颖。
《信息安全概论(第2版)》全面介绍了信息安全的基本概念、原理和知识体系，主要内容包括信息保密技术、信息认证技术、PKI与PMI认证技术、密钥管理技术、访问控制技术、网络的攻击与防范、系统安全、网络安全技术和信息安全管理等内容。

本书内容全面，既有信息安全的理论知识，又有信息安全的实用技术。
文字流畅，表述严谨，并包括信息安全方面的一些最新成果。
《信息安全概论(第2版)》可作为高等院校信息安全相关专业的本科生、研究生的教材或参考书，也可供从事信息处理、通信保密及与信息安全有关的科研人员、工程技术人员和技术管理人员参考。

<<信息安全概论>>

书籍目录

章节摘录

版权页：插图：· 首先B对文件的签名是合法的，和传统的签名具有相同的属性。
· B不能将所签文件与实际文件联系起来，即使他保存所有曾签过的文件，也不能获得所签文件的真实内容。
（2）盲签名完全盲签名可以使A令B签任何内容的文件，这对B显然是很危险的，例如，对“ B欠A100万元 ”这样的内容赋予完全盲签名显然是十分危险的。
因此完全盲签名并不实用。
为了避免这种恶意的使用，采用“ 分割一选择 ”技术，使B能知道所签的为何物，但仍保留了完全盲签名有意义的特征，即B能知道所签为何物，但是由于协议中规定的限制条件，使得B无法进行对他有利的欺诈，或者说进行欺诈所需代价超过其获利。
这就是肓签名的实用价值所在。
以下是两个著名的体现盲签名的例子。
例3-1要确定进出关口的人是不是毒贩，海关不可能对每个人进行检查。
一般用概率方法，例如对人关者抽取1/10进行检查。
那么毒贩在大多情况下可逃脱，但有1/10的机会被抓获。
而为了有效惩治犯罪，一旦抓获，其罚金将大于其他9次的获利。
所以通过适当地调节检查概率，就可以有效控制贩毒活动。
例3-2反间谍组织的成员身份必须保密，甚至连反间谍机构也不知道他是谁。
机构组织要给每个成员一个签名文件，文件上可能会注明：持此签署文件的人将享有充分的外交豁免权，并在其中写入该成员的化名。
每个成员有自己的不止一个的化名名单，使反间谍机构不能仅仅提供出签名文件，还要能验证提供签署文件的人是不是真正的合法组织成员。
特工们不想把他们的化名名单送给所属机构，因为敌方可能已经破坏了该机构的计算机。
另一方面，反间谍机构也不会盲目地对特工送来的文件都进行签名。
一个聪明的特工可能会送来这样的文件：“ 该成员已退休，每年发给100万退休金 ”，请求签名，若对这样内容的文件签名那不就麻烦了吗？
现在假定每个成员可有10个化名，他们可以自行选用，别人是不知道的。
假定成员并不关心在哪个化名下得到了豁免权，并假定机构的计算机为C，看下面的协议能有什么效果：①每个成员准备10份文件，各用不同的化名，以得到豁免权；②成员以不同的盲因子肓化每个文件；③成员将10个文件送给计算机C；④C随机选9个，并询问成员每个文件的盲因子；⑤成员将适当的盲因子送给C；⑥C从9个文件中移去盲因子，确信其正确性；⑦C将所签署的第10个文件送给成员；⑧成员移去盲因子，并读出他的新的化名Bob，这可能不是他用以欺诈的那个化名。
若他想用一个化名进行欺诈，成功的概率只有1/10。

编辑推荐

《信息安全概论(第2版)》是普通高等教育“十一五”国家级规划教材和信息安全专业系列教材之一。

版权说明