

<<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

出版单位：北京邮电大学

作者：牛少彰，崔宝江，

页数：255

字数：370000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<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

第1章 概述

1.1 信息的定义、性质和分类

1.1.1 信息的概念

1.1.2 信息的特征

1.1.3 信息的性质

1.1.4 信息的功能

1.1.5 信息的分类

1.2 信息技术

1.2.1 信息技术的产生

1.2.2 信息技术的内涵

1.3 信息安全概述

1.3.1 信息安全概念

1.3.2 信息安全属性

1.4 信息安全威胁

1.4.1 基本概念

1.4.2 安全威胁

1.4.3 网络攻击

1.5 信息安全的实现

1.5.1 信息安全技术

1.5.2 信息安全管理

1.5.3 信息安全与法律

1.5.4 网络的安全防范

小结

思考题

第2章 信息保密技术

2.1 古典密码

2.2 分组加密技术

2.2.1 基本概念

2.2.2 标准算法的介绍

2.2.3 分组密码的分析方法

2.3 公钥加密技术

2.3.1 基本概念

2.3.2 RSA公钥密码算法

2.3.3 ElGamal算法

2.3.4 椭圆曲线算法

2.4 流密码技术

2.4.1 流密码基本原理

2.4.2 二元加法流密码

2.4.3 几种常见的流密码算法

2.5 电子信封技术

2.6 信息隐藏技术

2.6.1 信息隐藏技术的发展

2.6.2 信息隐藏的特点

2.6.3 信息隐藏的方法

<<信息安全概论>>

2.6.4 信息隐藏的攻击

小结

思考题

第3章 信息认证技术

3.1 Hash函数和消息完整性

3.1.1 基本概念

3.1.2 常见的Hash函数

3.1.3 消息认证码

3.2 数字签名技术

3.2.1 数字签名的基本概念

3.2.2 常用的数字签名体制

3.2.3 盲签名和群签名

3.3 身份认证技术

3.3.1 基本概念

3.3.2 身份认证系统的分类

3.3.3 常见的身份认证技术

3.4 认证的具体实现

3.4.1 认证的具体实现与原理

.....

第4章 PKI与PMI认证技术

第5章 密钥管理技术

第6章 访问控制技术

第7章 网络的攻击与防范

第8章 系统安全

第9章 网络安全技术

第10章 信息安全管理

参考文献

<<信息安全概论>>

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。

这就是盲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盲化每个文件；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

本站所提供下载的PDF图书仅提供预览和简介, 请支持正版图书。

更多资源请访问:<http://www.tushu007.com>